ASPJ Africa and Francophonie

1st Quarter 2018 Volume 9, No. 1

AIM HIGH . . . FLY-FIGHT-WIN

AIR & SPACE POWER JOURNAL

ASPJ–Africa and Francophonie 1st Quarter 2018

ASPJ–Afrique et Francophonie 1er Trimestre 2018

The *Air and Space Power Journal* (ISSN 1931-728X), published quarterly, is the professional journal of the United States Air Force. It is designed to serve as an open forum for the presentation and stimulation of innovative thinking on military doctrine, strategy, force structure, readiness, and other matters of national defense. The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

http://www.af.mil

http://www.aetc.randolph.af.mil

http://www.au.af.mil

ASPJ–Africa and Francophonie
600 Chennault Circle
Maxwell AFB AL 36112-6010
USA
Fax: 1 (334) 953-1645
e-mail: aspj.french@us.af.mil

Visit *Air and Space Power Journal* online at http://www.airuniversity.af.mil/ASPJ/

ASPJ Africa and Francophonie
1st Quarter 2018 Volume 9, No. 1

Editor's Picks

Articles

Editorial

Editor's Picks

Peacebuilding: Assumptions, Practices and Critiques; Deterring and Dissuading Cyberterrorism; Is Cyber Deterrence an Illusory Course of Action?; Sharia as Desert Business: Understanding the Links between Criminal Networks and Jihadism in Northern Mali; and Foundations of Economic Theory: Money, Markets and Social Power

Professor Teresa Almeida Cravo posits that peacebuilding has become a guiding principle of international intervention in the periphery since its inclusion in the *Agenda for Peace* of the United Nations in 1992. She considers, in her article, "Peacebuilding: Assumptions, Practices and Critiques," that the aim of creating the conditions for a self-sustaining peace in order to prevent a return to armed conflict is, however, far from easy or consensual. The conception of liberal peace proved particularly limited, and inevitably controversial, and the reality of war-torn societies far more complex than anticipated by international actors that today assume activities in the promotion of peace in post-conflict contexts. With a trajectory full of contested successes and some glaring failures, the current model has been the target of harsh criticism and widespread skepticism. This article critically examines the theoretical background and practicalities of peacebuilding, exploring its ambition as well as the weaknesses of the paradigm adopted by the international community since the 1990s.

Dr. John Klein in "Deterring and Dissuading Cyberterrorism" hypothesizes that cyberterrorism, while being written about since the early 2000s, is still not fully understood as a strategic concept and whether such actions can be deterred is hotly contested. Some strategists and policy makers believe that acts of cyberterrorism, especially by non-state actors, may prove to be undeterrable. Yet the leadership of both state and non-state actors tends to act rationally and function strategically, and therefore they can, in fact, be deterred to some degree. Helping to shape the legitimate options following a significant cyber attack, the Law of Armed Conflict has salient considerations for the deterrence of cyberterrorism, particularly the principles of military necessity and lawful targeting. Furthermore, when

considered holistically and using all available means, deterrence combined with dissuasion activities can lessen the likelihood of cyberterrorism, while mitigating any consequences should such a cyber attack actually occur.

Mr. Emilio Iasiello ascertains that with the U.S. government acknowledgement of the seriousness of cyber threats, particularly against its critical infrastructures, as well as the Department of Defense officially labeling cyberspace as a war fighting domain, the Cold War strategy of deterrence is being applied to the cyber domain in "Is Cyber Deterrence an Illusory Course of Action?" However, he adds, unlike the nuclear realm, cyber deterrence must incorporate a wide spectrum of potential adversaries of various skills, determination, and capabilities, ranging from individual actors to state run enterprises. What's more, the very principles that achieved success in deterring the launch of nuclear weapons during the Cold War, namely the threat of severe retaliation, cannot be achieved in cyberspace, thus neutralizing the potential effectiveness of leveraging a similar strategy. Attribution challenges, the ability to respond quickly and effectively, and the ability to sustain a model of repeatability prove to be insurmountable in a domain where actors operate in obfuscation.

How can we understand the social and economic dynamics that enable the operative space of the militant networks in northern Mali? is a question raised by Ms. Rikke Haugegaard, in her article "Sharia as 'Desert Business': Understanding the Links between Criminal Networks and Jihadism in Northern Mali." This article argues that jihadist militant groups are actors in local power struggles rather than "fighters" or "terrorists" with extremist ideological motivations. She argues that the sharp distinctions drawn by the Malian government and the international community between compliant and non-compliant groups in the implementation of the peace agreement from June 2015 is problematic. She concludes that understanding the conflicts in northern Mali requires an increased focus on the links between jihadist militant groups, local politics and criminal network activities in Gao and Kidal.

In "Foundations of Economic Theory: Money, Markets and Social Power," CEO Garry Jacobs postulates that the future science of Economics must be human-centered, value-based, inclusive, global in scope and evolutionary in perspective. It needs to be fundamentally interdisciplinary to reflect the increasingly complex sectoral interconnections that characterize modern society. It must also be founded on trans-disciplinary principles of social existence and human development that constitute the theoretical foundation for all the human sciences. He emphasizes that markets and money are instruments for the conversion of social potential into social power. They harness the power of organization to transform human energies into the capacity for social accomplishment. The distribution of rights and privileges in society determines how these social institutions function and who benefits.

Rémy Mauduit, Editor
Air & Space Power Journal–Africa and Francophonie
Maxwell AFB, Alabama

Peacebuilding

Assumptions, Practices and Critiques

Teresa Almeida Cravo, PhD*

Peacebuilding has become a guiding principle of international intervention in the periphery since its inclusion in the United Nations' (UN) *Agenda for Peace* in 1992.[1] With the objective of creating the conditions for a self-sustaining peace in order to prevent a return to armed conflict, peacebuilding is directed towards the eradication of the root causes of violence and is necessarily a multifaceted project that involves political, legal, economic, social and cultural institutions and security practices, which are understood as complementary and mutually reinforcing.

However, the transition from armed violence to lasting peace has not been easy or consensual. The conception of liberal peace proved particularly limited, and inevitably controversial, and the reality of war-torn societies far more complex than anticipated by international actors that assume activities in the promotion of peace in post-conflict contexts today. With a career full of contested successes and some glaring failures, the current model has been the target of harsh criticism and widespread skepticism.

This article critically examines the theoretical background and practicalities of peacebuilding, exploring its ambition as well as the weaknesses of the paradigm adopted by the international community since the 1990s. In this sense, it first addresses the intellectual origins of the concept to then focus on its co-optation as a canon for UN action. The exploration of peacebuilding with regards to the institutionalized pattern of international interventionism is divided into three parts: assumptions, institutional practice and critical assessment. Its principles and objectives are discussed,

*Teresa Almeida Cravo is a researcher at the Centre for Social Studies, at the Humanities, Migration and Peace Studies Research Group, and an Assistant Professor in International Relations at the Faculty of Economics of the University of Coimbra. She is also currently co-coordinator of the PhD program "Democracy in the XXI[st] Century" at the University of Coimbra. She holds a PhD from the University of Cambridge, Department of Politics and International Studies.

The English translation of this article was funded by national funds through FCT—Fundação para a Ciência e a Tecnologia—as part of OBSERVARE project with the reference UID/CPO/04155/2013, with the aim of publishing on Janus.net. Text translated by Thomas Rickard.

Teresa Almeida Cravo, "Peacebuilding: Assumptions, Practices and Critiques," *JANUS.NET e-journal of International Relations* 8, no. 1 (May-October 2017), http://hdl.handle.net/11144/3032.

followed by a brief explanation of its implementation on the ground in terms of four dimensions—military and security, politico-constitutional, socio-economic, and psycho-social. The article finishes by reflecting on the recurrent and most damning criticisms of peacebuilding, highlighting the problems and limitations that have plagued this intervention model over the last twenty years.

Johan Galtung and the intellectual origins of peacebuilding

The concept of peacebuilding was introduced in the academic lexicon long before it became consensual in the world of policymaking. Johan Galtung, a Norwegian who is considered the founder of Peace Studies, first introduced this term in his 1976 article "Three Approaches to Peace: Peacekeeping, Peacemaking and Peacebuilding," setting the tone for the theoretical and operational exploration that would follow a few years later and which still remains prolific today.[2]

To understand the origins of the concept in question, we have to; however, take a step back in relation to the theoretical contribution of this author. The three approaches to peace developed in the article are intimately and directly related to his innovative proposal to redefine peace and violence, presented in the 1960s.[3] Galtung defines peace as the absence of violence; and defines violence as any situation in which human beings are being influenced so that their actual somatic and mental realizations are below their potential. This definition intended at the time to go beyond the dominant notion of violence as a deliberate act by an identifiable actor to incapacitate another, which the author considered too limited: "if this were all violence is about, and peace is seen as its negation, then too little is rejected when peace is held up as an ideal."[4] For conceptual clarification, Galtung begins by exploring a dual definition of peace: negative peace as the absence of violence and war and positive peace as the integration of human society.[5] Research for peace would be, in this perspective, the study of the conditions that bring us close to both, which ultimately produce what Galtung calls "general and complete peace."[6]

This conceptualization was not without criticism—particularly for being considered too vague and of no practical use—and, later, Galtung presents what can be considered as his greatest contribution to the theoretical assumptions of Peace Studies: the identification of the triangle of violence and the respective triangle of peace. In the triangle of violence the author distinguishes three aspects: direct violence, structural violence and cultural violence—the first two concepts presented in 1969 and the latter in 1990. For the author, direct violence is the intentional act of aggression with a subject, a visible action and an object. Structural violence is indirect, latent and deriving from the social structures that organize human beings and societies—for example, repression in its political form and exploitation in its economic form.[7] And lastly, cultural violence is a system of norms and underlying behaviors of, and which

legitimize structural and direct violence; that is, the social cosmology that allows one to look at repression and exploitation as normal or natural and, therefore, more difficult to uproot.[8] With this formulation, Galtung points out the problems and limitations of the definitions of violence that only cover social conflicts of a large scale (war), and encourages the understanding of peace in its broadest sense as a direct, structural and cultural peace, exposing and studying the global structural dynamics of repression and exploitation as well as the symbolic violence that exists in ideology, religion, language, art, science, law, the media and education.

It is not surprising, therefore, that the next step in the conceptual path of the Norwegian author was to confront this understanding with the concrete practice of international intervention, specifically in his article that develops the concepts of peacekeeping, peacemaking and peacebuilding. According to Galtung, peacekeeping constituted a "dissociative" approach, whose goal was the promotion of distance and a "social vacuum" between antagonists through the assistance of a third party.[9] This strategy is sinned for understanding conflict as an interruption of the *status quo* and for prescribing the return to *status quo ante* as a solution. It did not question whether this *status quo ante* should effectively be regained and preserved; it merely aimed for the maintenance of the absence of direct violence between actors in conflict, and therefore inadvertently contributed to continued structural violence.[10] Since the preservation of structural violence ultimately promotes direct violence—and thus the likely return to open conflict in the long term—this was not a satisfactory approach for Galtung.[11]

Peacemaking, on the other hand, represented a more comprehensive approach, anchored in conflict resolution, whose aim went beyond the cessation of hostilities to focus on ways to transcend inconsistencies and contradictions between parties.[12] However, while recognizing the potential "radicality" of the conflict resolution approach, Galtung claims that this is usually directed toward preservation, and not at the dispute of, the (violent) *status quo*, and oriented towards actors, and not necessarily to the system (structure), that (re)produces violence.[13] Peacemaking and conflict resolution are thus primarily understood as residing in the "minds of the conflicting parties" and achieved as soon as an agreement is signed and ratified—a conception that Galtung denounces as "narrow," "elitist," and negligent when considering the structural factors that are essential in building a sustainable peace.[14]

Galtung's understanding of peacekeeping and peacemaking leads him to develop a new concept: peacebuilding. Unlike the other two approaches, peacebuilding is *necessarily* an associative approach to conflict, able to cope with the direct, structural and cultural causes of violence in their broadest sense—and hence in line with his concept of positive peace. The removal of the root causes of violence would focus on principles such as "equity" (as opposed to domination/exploitation and towards horizontal interaction); "entropy" (as opposed to elitism and towards a sense of inclusion);

and "symbiosis" (as opposed to isolation and towards a sense of interdependence).[15] While acknowledging the difficulty and complexity above, Galtung's conception of peacebuilding is undoubtedly maximalist, ambitious and anchored in the idea of the struggle for peace as comprehensively covering "several fronts."[16]

This theoretical discussion proposed by Galtung on different ways of understanding violence and peace went far beyond a mere academic exercise—having had clear practical implications, especially once it was adopted by the UN in 1992, as we shall see below.

The theoretical assumptions of the model

Galtung's reflection inspired Boutros-Ghali, a United Nations Secretary-General enthusiastic about the prospect of a more dynamic and interventionist world organization, following the profound change in global affairs. It was essentially a combination of three factors that prompted a strong reaction from the international community and, in particular, the UN in the early 1990s. First, the end of the Cold War resulted in the easing of relations between the major powers within the Security Council and a renewed commitment to the founding principles of the organization, as well as the triumph of liberalism and its emphasis on human rights and democracy.[17] Second, the dramatic increase in the number of violent conflicts in the periphery, which affected 50 countries on different continents in 1991, finally gained visibility and prominence on the international agenda.[18] And lastly, the nature of these same conflicts—particularly devastating civil wars that challenged centralized state power, considered immoral and destabilizing for the regional and international system—created, mainly in the West, a public opinion favorable to interventionism.[19]

Taking advantage of this historic moment of "multilateral optimism" and facing these wars of the 1990s as "wars of the international community" that required the organization to respond with determination, Boutros-Ghali presented an ambitious proposal to address the challenges to international peace and security in the post-Cold War period, embodied in the *Agenda for Peace*.[20] This document practices an institutionalized model of peace that gives the UN a more consistent, dynamic and bolder remit, as well as a considerable increase in international importance in relation to previous decades.

There are four interrelated strategies proposed by the Secretary-General: preventive diplomacy, peacemaking, peacekeeping and, ultimately, peacebuilding.[21] Preventive diplomacy has two goals: first, to prevent a situation of latent conflict developing into a *de facto* violent situation; and, second, to contain the potential spread of a *de facto* situation of violent struggle to other regions and social groups. Peacemaking aims to support conflicting parties in peace negotiations toward an agreement, making use of the peaceful means contained in Chapter VI of the Charter of the United

Nations.[22] Peacekeeping involves sending UN forces—so-called peacekeepers—to the ground, after an agreement between parties and with their expressed consent, to stabilize volatile areas and ensure that the peace process is effectively fulfilled. Novelty is undoubtedly in the concept of "post-conflict peacebuilding," announced then as a new priority of the organization.

Objectives and principles

Defined as "action to identify and support structures to strengthen and solidify peace in order to avoid a return to conflict,"[23] peacebuilding thus encompasses two different but simultaneously complementary tasks: on the one hand, the negative task of preventing the resumption of hostilities; and on the other, the positive task of "addressing the root causes of the conflict."[24] This articulation closely follows Galtung's theoretical proposal on peace and violence discussed above that promotes a maximalist agenda for positive peace as essential to a lasting negative peace—that is the end of direct violence.[25] Boutros-Ghali is indeed clear in his ambition: the model he proposes ultimately wishes to deal with "economic despair, social injustice and political oppression" as sources of the violence plaguing the system.[26] And to achieve this goal, the UN stands ready and willing to be involved as an "external guarantee" at all stages of conflict situations.

The four strategies contained in the *Agenda for Peace* are therefore seen as complementary, where the various stages of the transition from violent conflict to peace share common goals that require an integrated approach. Peacebuilding begins to take shape within the framework of peacekeeping operations that are, in turn, sent to the ground as a result of negotiated peace agreements. Progressively, the responsibility of peacebuilding moves to nationals of countries emerging from conflict, with the help of external actors, so that foundations are built for a self-sustaining peace and, thus, new conflicts are prevented.

Reflections in individual reports that followed—among them, *Supplement to the Agenda for Peace,* 1995; the *Brahimi Report,* 2000; *United Nations Peacekeeping Operations: Principles and Guidelines*, 2008; and *Peacebuilding: an orientation,* 2010—continued to emphasize this idea of interconnection:

> peace operations are rarely limited to a single type of activity, and the boundaries between conflict prevention, peace-making, peacekeeping, peacebuilding and peace enforcement have become increasingly diffuse, highlights the 2008 report.[27]

Peacebuilding is understood as a preventive tool,[28] essential to "heal the wounds" of conflict[29] and significantly reduce the risk of return to hostilities.[30] Peacekeeping and peacebuilding are dubbed "inseparable partners"[31] and peacekeepers as "early peacebuilders,"[32] since peacebuilding cannot act without peacekeeping and the latter does not have an exit strategy without the first. In other words, the central idea, then,

is of *continuum*: between negative peace and positive peace, between stabilization and development, and between structural prevention and consolidation.

Liberal peace

If the adoption of a *maximalist* vision of peace—coinciding with Galtung's theoretical proposal—was clearly due to the intellectual and political environment triggered by the end of the Cold War, the specific *conception* of the model to implement in conflict zones also reflected those who emerged triumphant from the bipolar confrontation.

In fact, the approach that gave shape to this new ambition to promote peace in the periphery, and was subsequently integrated in the new collective security instruments, was the Western approach of so-called liberal peace.[33] As explained by Christopher Clapham, the winners of the bipolar conflict—not only capitalist, liberal democracies but also their civil societies, and the great mass of non-governmental organizations and international institutions that they control—sought to restructure the international system in accordance with the values that emerged victorious at that time[34] and presented liberal democracy and the market economy as the "global recipe for development, peace and stability."[35]

In relation to this, Roland Paris states that peace building is effectively "an enormous experiment in social engineering—an experiment that involves transplanting Western models of social, political and economic organization into war-shattered states in order to control civil conflict: in other words, pacification through political and economic liberalization."[36] The fall of the Communist Bloc and its alternative model meant that this interventionist approach was readily encouraged, and it was imposed without rival in the four corners of the world—something Pierre Lizée calls the "end of history syndrome."[37] By introducing political and economic conditionalities through peace operations and development assistance programs, the model of market democracies spread throughout the Third World.[38]

The great potential for opening the concept of peacebuilding to numerous definitions based on different understandings and approaches—which could have gained a multitude of concrete forms in post-conflict contexts—was instead reduced to the specificity of the Western and liberal worldview, and therefore closed to other experiences and alternatives.

The model in practice

There was, since its beginning, a convergence around what Miles Kahler called the "New York Consensus,"[39] despite the absence of a central organ for all peacebuilding activities within the UN during the first decade, on the one hand, and the

constant presence of several other international actors who arrogated responsibilities under international interventions on the other. The "New York Consensus" reflected the *liberal dream* of creating multiparty democracies with market economies and strong civil societies, as well as promoting Western liberal practices and values, such as secular authority, centralized governance, the rule of law and respect for human rights.[40]

As Oliver Richmond explains, peace is thought by the Western international community as an "achievable ideal form, the result of top-down and bottom-up actions, resting on liberal social, political and economic regimes, structures and norms."[41] To think of "peace as governance"[42] also involves looking at peacebuilding as a means to an end: that is, as an institutionalized model embodied in a set of steps needed to build liberal peace. No wonder, therefore, that the practice of peacebuilding has involved a standardized framework for action that sought to take on a universal and hegemonic character.

Multidimensionality

It is the involvement of the UN in Namibia in 1989 that represents the first attempt to implement this paradigm. This peace operation goes far beyond the traditional supervision of ceasefires and is mandated to assist the establishment of democratic political institutions as well as monitor elections that would ensure the country's independence. The relative success of the mission attested the organization's capacity and willingness to undertake more ambitious and large-scale peace operations, with activities going far beyond those until then undertaken, and in a variety of countries emerging from armed conflicts in Asia, Africa, Europe and Central America.[43] We therefore witnessed, during the nineties, a dramatic expansion of the liberal peace model that Oliver Ramsbotham calls the "UN's post-settlement peacebuilding standard operating procedure,"[44] which is embodied, on the ground, by four interdependent dimensions: (1) military and security, (2) politico-constitutional, (3) socio-economic and (4) psycho-social.

The military and security dimension

The security dilemma that assaults groups involved in intrastate conflicts is considerably higher than among countries involved in interstate conflicts, to the extent that the strengthening of state authority involves the recovery of the monopoly of the legitimate use of force and control of the entire territory; that is, it entails precisely the reconstitution of a central political power with the capacity to impose itself over the remaining political and military powers. It is therefore necessary to institutionalize safeguards to neutralize the understandable feeling of insecurity that pervades the various actors who fear exclusion and fear that the centralization of political and

military power favors the opposing group to their detriment. The military and security dimension of the peacebuilding model therefore has two objectives: to establish a balance between the warring parties and to restrict the ability of combatants to return to hostilities. There is, accordingly, a program specifically aimed at soldiers, which includes the standardized phases known as "DDR": (1) demobilization, (2) disarmament and (3) reintegration into civilian life or the national armed forces.[45]

The international community's attention is later focused on security sector reform (SSR), which covers military, police and intelligence services, and seeks to establish more transparent, efficient and democratic control.[46] Pointing to a generic notion of good governance and the rule of law, SSR is a long-term, comprehensive approach, concerned not only with the *capacity* to provide security to citizens but also *accountability* through civil and democratic supervision.[47]

The politico-constitutional dimension

This dimension seeks to carry out a political transition that involves the legitimation of government authority; reform of the State's administration dismantled during the conflict; and the transfer of tensions among conflicting groups to the institutional level—that is the idea of politics as a continuation of the conflict through non-violent means, a notion which comes from Michel Foucault and that Ramsbotham calls "Clausewitz in reverse."[48]

The political regime that underlies these changes is liberal democracy, which is considered more prone to peace both internally and internationally.[49] As the "dominant political philosophy"[50] of the international post-Cold War community, it was successively promoted and imposed on intervened societies, focusing primarily on reform and promotion of the rule of law and of those elements with the most impact on the process of democratization and the creation of a democratic culture: political parties, media and civil society.

The introduction of this democratic model in post-conflict scenarios can, however, take different forms. A first approach was to hold short-term multi-party elections, which symbolized the immediate responsibility of national actors and the legitimacy of new political power (such as in Angola in 1992). The winner-takes-all logic of the zero-sum game in highly unstable contexts led, however, to the emergence of a second approach considered less destabilizing: coalition governments, which aimed to socialize actors in terms of sharing negotiated power and the practice of consensus before holding first elections (e.g., in Afghanistan in 2002). One last way—only for cases where there is a large commitment from the international community in terms of financial provisions, human resources and time—is the "international protectorate," in which the transitional administration is upheld by an external actor (e.g., East Timor with the UN between 1999 and 2002).

The socio-economic dimension

This dimension aims to reverse the particularly devastating impact of armed conflict on a country's socio-economic fabric, drawing upon international financial aid. Following a *continuum* between relief, recovery and development,[51] the international community usually begins with humanitarian aid and also has a crucial role in medium- to long-term support for the reconstruction of basic infrastructure and the application of macroeconomic stabilization policies. It should be noted that the understanding of this economic recovery, as well as monetary and fiscal (im)balances, has been guided by neoliberal ideology.[52] During the eighties and nineties, this economic philosophy materialized in the so-called structural adjustment programs, applied all over the developing world by international financial institutions loyal to the so-called "Washington Consensus."[53] These economic policies advocated liberalization, privatization and deregulation of countries' economies, opening them to the market; they were accompanied by weakening and concomitant cutbacks in the interventionist role of the State in a context of strict fiscal discipline and tax reform aimed at attracting foreign investment.

Devastating criticism of this neoliberal model related to difficulties in favorably integrating these post-conflict economies into the world market and in a sustainable manner led to strong calls for the easing of economic practices, the regaining of the State as a development agent and the need to reconcile the imperatives of short-term stabilization and long-term imperatives of growth and development.[54] In general, however, the reforms of the "post-Washington Consensus" that followed, mainly in the late 1990s, were towards a "neoliberal-light package" rather than a real challenge to the model's assumptions.

The psycho-social dimension

One of the most serious costs of war is the enduring nature of the impact of the culture of rooted violence in societies plagued by conflicts over a long period.[55] The restoration of the social fabric of war-torn countries depends on the deconstruction of stereotypes and the conditions that fueled the conflict and polarized communities, requiring, therefore, a change of individual attitudes and, more generally, the behavior of society as a whole towards reconciliation.

Different societies have dealt with their psycho-social trauma resulting from conflicts in different ways. Some opted for what we call here the "Amnesia formula," that is burying the past, through amnesties lest to cause instability. This path is difficult to follow since sufferers are normally cursed with good memory. There are fundamentally three other recurring practices in dealing with the past in these contexts (which may exist simultaneously or even be associated with amnesty laws): through (1) truth and reconciliation commissions, as in El Salvador; (2) the courts (judicial

settlement, either domestically or internationally), such as in Rwanda; and (3) traditional reconciliation practices (rituals entirely dependent on local cultural resources), as in East Timor. This is, ultimately, a painful and slow process that involves readapting to each other and rebuilding peaceful relations. Reconciliation in its broadest sense is thus ultimately the end goal of a transition to peace.

Consensus on peacebuilding's institutional practice was generalized. The global organization sought to strengthen it and streamline monitoring missions through administrative reforms such as the creation of the Department of Peacekeeping Operations as early as 1992, and also through the more systematic use of the Special Representatives of the Secretary-General. In particular, the creation of the Peacebuilding Commission in 2005 intended to fill an institutional gap with regards to the UN's capacity to act in contexts of violence and state fragility, as well as to learn from its mistakes and best practices within a framework of liberal peace.

Given the growing complexity of threats to international peace and security, the logic of complementarity between the work of the UN and multiple regional organizations and civil society also gained momentum. Putting into practice what had been envisaged by Chapter VIII of the UN Charter, partnerships with regional organizations—considered a privileged space for crisis resolution and peace promotion—became stronger. Institutions such as the OECD, the EU, NATO and the African Union began to play an increasing role in peacebuilding, following, in general, the institutionalized model. In particular, the enlargement of both NATO and the EU on the European continent and, subsequently, the expansion of their operations beyond Europe intensified the application of the paradigm and further legitimized the liberal peace model as a standard action. Simultaneously, the prominence on the international agenda of the concept of human security and subsequent appeals for intervention provided more space for civil society organizations in the discourse and practice of peace and conflict.[56] Viewed as more focused on individuals and tending to be bottom-up in their approaches, these organizations gained momentum and their participation in the various stages of the promotion of peace have become regarded as essential to the success of a sustainable peace process. As pointed out by Edward Newman et al., this understanding of both the challenge and the most appropriate response, which quickly spread to other organizations, reflects not only the dominant consensus but also normative progress towards weakening the inviolability of territorial integrity and, concomitantly, the growing acceptance of international interventionism.[57]

Criticism of the model

Expectations for this new era of global interventionism were high and soon dashed, giving rise to widespread pessimism, in large part because of the dramatic and

newsworthy failures of missions in Angola, Bosnia, Somalia and Rwanda. Statistics on the recurrence of violent conflicts in societies previously ravaged by war—about 50 per cent in the first five years following the signing of peace agreements—led to the favored model being openly questioned.[58] But even where there was no blatant return to hostilities, the materialization of formal peace faced serious difficulties and, in many cases, the initial effusive statements of *success* proved premature.[59]

The main protagonist of this ambitious interventionist project attracted much of the responsibility for the setbacks and failures. In fact, the complexity of the problems faced in peace and security with the end of the Cold War egregiously defied the institutional capacity of UN missions of this scale on several levels: financial resources; qualified and experienced staff; information gathering and planning; communication; coordination; and operational knowhow.[60] The undeniable difficulty of operationalization of the UN proposal—evident right from the start—confirmed glaring weaknesses and difficult dilemmas that were undermining the credibility, legitimacy, and intervention capacity of the organization.

It would, however, be criticism of the model of peacebuilding itself, advocated both by the UN and by other more interventionist actors of the international system; that would prove to be more forceful. Of these, it is possible to distinguish two groups of critics through their analytical positions: (1) reformist critiques (the problem-solvers)[61] —who, while recognizing relevant defects in the model, advocate its continuation, refining the process without challenging its ideological foundation; and (2) structural critics—who question the legitimacy of the model itself, its values, interests and the reproduction of hegemonic relations, challenging, thus, the order accepted as an immutable reality.

More and better interventionism: the reformist critiques

Both in terms of numbers and influence in the world of policymaking, most authors who focus on the theme of promoting peace in peripheral States belong to the so called mainstream and may be labelled problem-solvers. They are authors who advocate the existing order and whose concern is to increase the practical relevance and efficiency of the liberal peace model.[62] Believing ultimately that, despite the disappointing results, external intervention is more beneficial than harmful and that the alternative is the abandonment of millions of people from the periphery to a condition of insecurity and violence, this line of thinking accuses the "hyper-critics" of widespread skepticism and focuses on the improvement of the model in order to minimize its destabilizing effects and improve its capabilities.[63]

Roland Paris and Timothy Sisk generally represent this position and point to five contradictions inherent in the model that hinder its applicability: (1) external

intervention is used to promote self-government; (2) international control is required to create local ownership; (3) universal values are promoted to tackle local problems; (4) the break with the past is concomitant with the affirmation of history; and (5) short- and long-term imperatives often conflict.[64] These tensions materialize in practical challenges to peacebuilding in the field of: (1) international presence (i.e. the degree of interference in the internal affairs of the host State—size of the mission, nature of the tasks, consent versus compliance/enforcement, combination of violent and/or non-violent means); (2) duration of the mission (post-war reconstruction as necessarily a long-term activity versus accountability of national actors); (3) local participation (elites versus population, international priorities versus local priorities); (4) dependence (on international actors versus self-sustaining peace); and (5) consistency (organizational coordination and normative clout).[65]

The realization of these dilemmas does not lead to rejection of this kind of response from the international community; on the contrary, this analysis is seen as a "realistic" way of trying to *manage* contradictory imperatives in order to improve performance and efficiency of missions, adjust expectations and thus "save" the liberal peace project.[66] The ideological foundations of liberal peace in transforming countries devastated by civil wars into liberal market democracies are therefore not questioned. Over the years, the incorporation of reformist critiques entailed only some adaptation in terms of methodology, with the adoption of more gradual reforms—"institutionalization before liberalization"—in order to build and strengthen autonomous governance institutions that are effective and legitimate before the introduction of winner-takes-all elections and drastic reforms to open up markets.[67] This strategy, more sensitive to the adverse effects of "shock therapy," maintained, however, the two global goals governing the implementation of the paradigm since the early nineties: (1) the reproduction of the Western Weberian State in the periphery—with the strengthening of the SSR, the rule of law and good governance (the three most prominent pillars of the model in its second decade); and (2) the integration of these spaces in the world capitalist economy—generally preserving the neoliberal framework, while safeguarding against its most devastating socio-economic impact by supporting development and poverty reduction programs.[68]

The challenge to the global power structure: structural critiques

Structural critiques are mainly concerned with the ideology behind the thought and practice of peacebuilding and what this (re)produces in terms of the functioning of the international system. Unlike the perspective analyzed above, the aim of the authors is transformative, looking to explicitly resist hegemonic forms of power.[69] This normative commitment aims to transform the model itself—as opposed to an

adjustment in line with the preservation of the dominant paradigm of liberal peace (as well as the broader system of power relations)—as opposed to the preservation of the *status quo*.

Among the sharpest critiques are those who emphasize the Western hegemonic model of peacebuilding and its hierarchical, centralized and elitist nature. From a postcolonial perspective, liberal peace is understood as promoting Western culture, identity and norms over others.[70] The analogies between the peacebuilding and colonialism are therefore recurrent, considering both as contributing to power asymmetries between the Global North and the Global South. The structural problems of the design and implementation of peacebuilding models are thus seen in their relationship with the inequality of the international system: interventions impose a top-down model, create and reinforce a clear hierarchy between interveners and the intervened and act as an instrument of global governance of the West in the periphery, consolidating its hegemony, defending its geostrategic interests and promoting its values.[71] Its function is then the legitimacy of the world order which followed the victory of the Western Bloc in the Cold War, while serving the interests of Western states and international financial institutions controlled by them. Furthermore, the supposed *technical* solutions proposed and imposed by the Global North, such as the neoliberal strategies of post-war reconstruction, reproduce the conditions of conflict and cause the very violence they intend to solve, ultimately contributing to the system's instability.[72]

Looking to overcome this logic of the international imposing on the local, several authors have more recently explored the idea of a "post-liberal peace" model. The contribution, for example, of Oliver Richmond and Roger Mac Ginty focuses mainly on the theory of hybrid peace, where peace is a cumulative and long-term hybrid of endogenous and exogenous forces.[73] Refusing both the universality of liberal peace (as a principle and practice) as well as the romanticized "purity" of the local, the hybrid perspective notes local agency in resisting, subverting, renegotiating, ignoring, delaying and producing alternatives to the current paradigm. Recognition of this heterogeneity opens the way to think about Southern epistemologies and, in particular, about forms of State-building and societal governance that are distinct from those proposed by the hegemonic model.[74] The central idea is that, paying attention to worldviews that are culturally different from the Western; is it possible to recognize and create a multiplicity of "peaces" that are not exhausted by the overwhelming hegemony of liberal peace?

Notwithstanding their different characteristics and intentions, these critiques effectively put in question: (1) the *goodwill* of the intervention model—drawing attention to the imperialist features of the paradigm and the way it serves the interests and particular agendas of Northern countries in the South; (2) its nature—challenging the centrality of security (which favors order and stability at the expense of emancipation) and its elitist, technocratic and standardized essence; (3) its legitimacy—

questioning the presumption of the universality of Western liberalism as well as its Eurocentric, imposing and curtailing approach to local participation; and (4) its efficacy—stressing the maintenance of conflicting relationships, dependency on external actors and the adverse consequences of downplaying endogenous contributions.

Conclusion

There is no doubt that the model of peacebuilding undertaken by the various actors who today take the lead in international interventionism is a particularly ambitious project. From the mere freezing of armed conflicts, we have moved rapidly to attempt to settle their root causes through an institutionalized paradigm that dramatically changed the objectives and traditional functions of promoting peace in the periphery.

The results of this interventionist project were, however, far short of the desired, particularly for those who enthusiastically foresaw a new era able to solve the challenges to international peace and security of the post-Cold War. Two decades of internal and external criticism of the peacebuilding model did produce some reforms towards a *modus operandi* that is occasionally more flexible and more sensitive to other approaches. These adjustments did not, however, truly question the cultural and ideological assumptions of this paradigm, neither the global North's interests underlying the international action in conflict and post-conflict contexts. In fact, they could not even suitably solve most of the problems identified by the problem-solvers, as shown by the successive reports and assessments of peace operations led by international actors themselves. Indeed most of the criticism over the past twenty years remains valid today.

The appreciation of peacebuilding as a response to extreme levels of violence plaguing the system cannot, in this sense, fail to reveal an impact that is at least disappointing and often counterproductive. Although praising the will to go beyond the militarized model of negative peace—as well as how the fact translates into a renewed commitment of the international community towards the periphery devastated by violence and in need of help—skepticism about international efforts have clearly been justified. Serious limitations in the way the concept has been conceived and materialized on the ground—to which complaints can be added regarding the agendas and interests that are truly served with these interventions—are particularly serious problems that are still, in fact, far from being resolved.

Notes

1. United Nations, "An Agenda For Peace," 31 January 1992, http://www.un-documents.net/a47-277.htm.
2. Johan Galtung, "Violence, Peace and Peace Research," *Journal of Peace Research* 6, no. 3 (1969): 168.

3. For a more detailed analysis of Galtung's conceptual contribution see Teresa Almeida Cravo, "Os Estudos para a Paz," in *Segurança Contemporânea*, eds. Duque; Noivo & Almeida e Silva (Lisboa: PACTOR–Edições de Ciências Sociais e Política Contemporânea, 2016), 69-84.

4. Ibid.

5. Johan Galtung, "An Editorial," *Journal of Peace Research* 1, no. 1 (1964): 1-4.

6. Ibid, 2.

7. Galtung, "Violence, Peace and Peace Research."

8. Johan Galtung, "Cultural Violence," *Journal of Peace Research* 27, no. 3 (1990): 291-305.

9. Johan Galtung, "Three Approaches to Peace: Peacekeeping, Peacemaking and Peacebuilding," in *Essays in Peace Research*, Volume II, ed. Johan Galtung, (Copenhagen: Ejlers, 1976), 282.

10. Ibid., 283-284.

11. Ibid., 288.

12. Ibid., 290.

13. Ibid., 294-296.

14. Ibid., 296-297.

15. Ibid., 298-300.

16. Ibid., 104.

17. Hugh Miall, Oliver Ramsbotham, and Tom Woodhouse, *Contemporary Conflict Resolution* (Cambridge: Polity Press, 1999), 2; Peter Viggo Jakobsen, "The transformation of United Nations Peace Operations in the 1990s: Adding Globalization to the Conventional 'End of the Cold War Explanation," *Cooperation and Conflict* 37, no. 3 (2002): 267-282.

18. Peter Wallensteen and Margareta Sollenberg, "Armed Conflict, 1989-2000," *Journal of Peace Research* 38, no. 5 (2001): 632.

19. Mohammed Ayoob, "State-Making, State-Breaking and State Failure: Explaining the Roots of 'Third World' Insecurity," in *Between Development and Destruction. An Enquiry into the Causes of Conflict in post-Colonial States*, eds. Goor et al. (London: Macmillan Press Ltd, 1996), 67-90.

20. Teresa Almeida Cravo, "Duas décadas de consolidação da paz: as críticas ao modelo das Nações Unidas," *Universitas: Relações Internacionais - UniCEUB* 11, no. 2 (2013): 21-37.

21. United Nations, "An Agenda For Peace."

22. Ibid., para 42-45. The "Agenda for Peace" also refers to peace enforcement, included in the UN Charter, as an instrument available within this new framework for action.

23. Ibid., para 21.

24. Ibid., para 15.

25. Oliver Ramsbotham, "Reflections on UN Post-Settlement Peacebuilding," in *Peacekeeping and Conflict Resolution*, eds.Woodhouse & Ramsbotham (London: Frank Cass Publishers 2000), 171, 175.

26. United Nations, "An Agenda For Peace," para 15.

27. UN Department of Peacekeeping Operations, *United Nations Peacekeeping Operations: Principles and Guidelines*, (New York: United Nations Secretariat, 18 January 2008), 18, http://www.un.org/en/peacekeeping/documents/capstone_eng.pdf.

28. UN General Assembly Security Council, "Supplement to an Agenda for Peace: Position Paper of the Secretary-General on the Occasion of the Fiftieth Anniversary of the United Nations," 3 January 1995, para 47, http://www.un.org/documents/ga/docs/50/plenary/a50-60.htm.

29. Ibid., para 53.

30. UN Peacebuilding Support Office, *UN Peacebuilding: An Orientation*, (New York: Peacebuilding Support Office, September 2010), para 13, http://www.un.org/en/peacebuilding/pbso/pdf/peacebuilding_orientation.pdf.

31. UN General Assembly Security Council, "Report of the Panel on United Nations Peace Operations (Brahimi Report)," 21 August 2000, para. 28, http://www.un.org/documents/ga/docs/55/a55305.pdf.

32. UN Peacebuilding Support Office, *UN Peacebuilding: An Orientation*, p. 9.

33. Michael Doyle, "Three Pillars of the Liberal Peace," *American Political Science Review* 99, no. 3 (2005): 463-466.

34. Christopher Clapham, "Rwanda: The Perils of Peacemaking," *Journal of Peace Research* 35, no. 2 (1998): 193-194.

35. Alexandros Yannis, "State Collapse and its Implications for Peace-Building and Reconstruction," *Development and Change* 33, no. 5 (2002): 825.

36. Roland Paris, "Peacebuilding and the Limits of Liberal Internationalism," *International Security* 22, no. 2 (1997): 56.

37. Pierre Lizée, *Peace, Power and Resistance in Cambodia. Global Governance and the Failure of International Conflict Resolution*, (London: Macmillan Press Ltd., 2000).

38. Jakobsen, "The transformation of United Nations Peace Operations."

39. Miles Kahler, "Statebuilding After Afghanistan and Iraq," in *The Dilemmas of Statebuilding: Confronting the Contradictions of Postwar Peace Operations*, eds. Paris & Sisk (London: Routledge, 2009), 287-303.

40. Edward Newman et al., "Introduction," in *New Perspectives on Liberal Peacebuilding*, eds. Newman et al. (Tokyo: United Nations University Press, 2009), 12.

41. Oliver Richmond, *The Transformation of Peace* (London: Palgrave Macmillan, 2005), 110.

42. Ibid., 52-84.

43. Sonia Han, "Building a Peace that Lasts: The United Nations and Post-Civil War Peacebuilding," *New York University Journal of International Law and Politics* 26, no. 4 (1994): 842-845.

44. Oliver Ramsbotham, "Reflections on UN Post-Settlement Peacebuilding," 170.

45. UN General Assembly, "Disarmament, Demobilization and Reintegration Programs," 2 March 2006, para. 29-37, http://www.undp.org/content/dam/undp/documents/cpr/documents/ddr/SG_Report_on_DDR_to_GA_s-60-705_March_2006.pdf.

46. Mark Sedra, ed., *The Future of Security Sector Reform* (Ottawa: Centre for Governance Innovation, 2010).

47. On the link between peacebuilding, the rule of law and SSR see Teresa Almeida Cravo, "Linking Peacebuilding, Rule of Law and Security Sector Reform: The European Union's Experience," *Asia-Europe Journal* 14, Special Issue: The Rule of Law as a Strategic Priority in the European Union's External Action, no.1 (2016):107-124.

48. Ramsbotham, "Reflections on UN Post-Settlement Peacebuilding," 172.

49. For the democratic peace theory see Jarrod Hayes, "The Democratic Peace and the new Evolution of an old Idea," *European Journal of International Relations* 18, no. 4 (2012): 767-791.

50. Samuel Barnes, "The Contribution of Democracy to Rebuilding Postconflict Societies," *American Journal of International Law* 95, no. 1 (2001): 86.

51. Joanna Macrae and Nicholas Leader, "Apples, Pears and Porridge: The Origins and Impact of the Search for 'Coherence' between Humanitarian and Political Responses to Chronic Political Emergencies," *Disasters* 25, (2001), 155, doi:10.1111/1467-7717.00179.

52. David Harvey, *A Brief History of Neoliberalism* (Oxford: Oxford University Press, 2005).

53. John Williamson, "A Short History of the Washington Consensus," in *The Washington Consensus Reconsidered: Towards a New Global Governance*, eds. Serra & Stiglitz (Oxford: Oxford University Press, 2008), 14-30.

54. John Stiglitz, "Is there a Post-Washington Consensus Consensus?," in *The Washington Consensus Reconsidered: Towards a New Global Governance*, eds. Serra & Stiglitz (Oxford: Oxford University Press, 2008), 41-56.

55. John Paul Lederach, "Civil Society and Reconciliation," in *Turbulent Peace. The Challenges of Managing International Conflict*, eds. Crocker et al. (Washington, D.C.: United States Institute of Peace Press, 2001), 841-854.

56. UN Development Programme, *Human Development Report 1994*, (New York: Oxford University Press, 1994), http://hdr.undp.org/en/content/human-development-report-1994.

57. Newman et al., "Introduction," 5.

58. Paul Collier et al., *Breaking the Conflict Trap: Civil War and Development Policy* (New York: Oxford University Press and World Bank, 2003), 83.

59. See, for example, criticism of operations in Mozambique in Jeremy Weinstein, "Mozambique: A Fading U.N. Success Story," *Journal of Democracy* 13, no. 1 (2002): 141-156; and Cambodia in Pierre Lizée, *Peace, Power and Resistance in Cambodia.*

60. Adam Roberts, Benedict Kingsbury, eds., *United Nations, Divided World: the UN's Roles in International Relations* (Oxford: Clarendon Press, 1993).

61. For the concept of "problem-solver" see Robert Cox, "Social Forces, States and World orders: Beyond International Relations Theory," in *Neorealism and Its Critics*, ed. Keohane (New York: Columbia University Press, 1986), 204-254.

62. See, for example, Francis Fukuyama, *State-building: Governance and World Order in the 21st Century* (Ithaca, NY: Cornell University Press, 2004); Roland Paris, *At War's End: Building Peace after Civil Conflict* (Cambridge: Cambridge University Press, 2004); Michael Doyle and Nicholas Sambanis, *Making War & Building Peace* (Princeton: Princeton University Press, 2006); Charles Call and Elizabeth Cousens, "Ending Wars and Building Peace: International Responses to War-Torn Societies," *International Studies Perspectives* 9, (2008): 1-21; and Anna Jarstad and Timothy Sisk, eds., *From War to Democracy: Dilemmas of Peacebuilding* (Cambridge: Cambridge University Press, 2008).

63. Roland Paris, "Saving Liberal Peacebuilding," *Review of International Studies* 36, no. 2 (2010): 337-365.

64. Roland Paris and Timothy Sisk, eds., *The Dilemmas of Statebuilding: Confronting the Contradictions of Postwar Peace Operations* (London: Routledge, 2009).

65. Ibid., 306-309.

66. Paris, "Saving Liberal Peacebuilding."

67. Paris, *At War's End*, 179.

68. Graham Harrison, *The World Bank and Africa: The Construction of Governance States* (London: Routledge, 2004).

69. See, for example, Mark Duffield, *Global Governance and the New Wars. The Merging of Development and Security* (London: Zed Books, 2001); Michael Pugh, "The Political Economy of Peacebuilding: A Critical Theory Perspective," *International Journal of Peace Studies* 10, no. 2 (2005): 23-42; David Chandler, *Empire in Denial: The Politics of State-building* (London: Pluto, 2006); Oliver Richmond, "The problem of peace: Understanding the 'liberal peace'," *Conflict, Security & Development* 6, no. 3 (2006): 291-314; and Philip Darby, 'Rolling Back the Frontiers of Empire: Practising the Postcolonial', *International Peacekeeping* 16, no. 5 (2009): 699-716.

70. Kristoffer Lidén, "Peace, Self-governance and International Engagement: From Neo-colonial to Post-colonial Peacebuilding," in *Rethinking the Liberal Peace: External Models and Local Alternatives*, ed. Tadjbakhsh (New York: Routledge, 2011), 57.

71. David Chandler, "The Uncritical Critique of Liberal Peace," *Review of International Studies* 36, no. 1 (2010): 137-155.

72. Duffield, *Global Governance and the New Wars*; Pugh, "The Political Economy of Peacebuilding."

73. Oliver Richmond, *A Post-Liberal Peace: The Local Infrapolitics of Peacebuilding* (London: Routledge, 2011); and Roger Mac Ginty, *International Peacebuilding and Local Resistance: Hybrid Forms of Peace* (Basingstoke: Palgrave Macmillan, 2011).

74. Boaventura Sousa Santos, *Epistemologies of the South* (Boulder: Paradigm, 2014).

Deterring and Dissuading Cyberterrorism

John J. Klein, PhD*

Since the beginning of his Administration, President Barack Obama has stated that cybersecurity is one of the most important challenges facing the United States.[1] In doing so, he noted the irony that the very technologies used by the United States that enable great achievements can also be used to undermine its security and inflict harm on its citizens. For instance, the same information technologies and defense systems that make the U.S. military so advanced are themselves targeted by hackers from China and Russia, potentially leading to increased vulnerabilities. Consequently, ongoing and persistent cyber attacks are considered a threat to U.S. national security.[2]

Included in this overall cybersecurity challenge that President Obama addressed is the threat posed by cyberterrorism. Unfortunately, while being written about since the early 2000s, cyberterrorism is a concept whose definition is still not fully agreed upon. Confusion over cyberterrorism stems, in part, from recent attempts to stretch the concept to include hacktivism and terrorists' use of the Internet to facilitate conventional terrorist actions.[3] Furthermore, some strategists and policy makers believe that acts of cyberterrorism, by either states or non-state actors, may prove to be undeterrable.[4]

This view, however, is incorrect or, at best, a half-truth.[5] Based upon the lessons of history and how conflict in the other media of warfare has unfolded, the credible threat of overwhelming force or other severe actions can, under the right conditions, deter potential attackers from initiating a path of direct confrontation.

---

*John J. Klein is a Senior Fellow at Falcon Research in Northern Virginia. He holds a PhD in politics, with a strategic studies focus, from the University of Reading and a master's in national security and strategic studies from the U.S. Naval War College, where he was a Mahan Scholar. He previously served as a Federal Executive Fellow at the Brookings Institution in its Foreign Policy Studies program. Dr. Klein writes frequently on national policy, military strategy, and the implications of the Law of Armed Conflict.

The views expressed in this article are solely those of the author and do not necessarily reflect those of Falcon Research or those of the United States Government.

John J. Klein, "Deterring and Dissuading Cyberterrorism," *Journal of Strategic Security* 8, no. 4 (2015): 23-38. DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460 Available at: http://scholarcommons.usf.edu/jss/vol8/iss4/2

Cyberspace and Cyberterrorism

The cyber domain, or cyberspace, has been defined by Andrew Krepinevich as:

> [the world's] computer networks, both open and closed, to include the computers themselves, the transactional networks that send data regarding financial transactions, and the networks comprising control systems that enable machines to interact with one another.[6]

As such, the cyber domain utilizes expansive lines of communication involving a global network, along with hubs of activity at server farms or network hardware locations.[7] Cyber activities involve international commerce and finance, social media, information sharing, and more recently, military-led activities.[8]

When considering whether or how acts of terrorism in the cyber domain can be deterred, the definition of cyberterrorism provided by Dorothy Denning in 2000 before the House Armed Services Committee proves useful:

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[9]

Under this "severity of effects" determination, computer attacks that are limited in scope, but that lead to death, injury, extended power outages, airplane crashes, water contamination, or major loss of confidence in portions of the economy may also qualify as cyberterrorism.[10]

When considering the definition above, cyberterrorism does not include acts of hacktivism. *Hacktivism* is a term used by many scholars to describe the marriage of hacking with political activism.[11] Similar to the actions of hackers, hacktivism includes activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software. Differing from hacktivists, those considered solely as hackers do not necessarily have political agendas.[12]

Hacktivism, though motivated for political reasons, does not amount to cyberterrorism. While hacktivists typically seek to disrupt Internet traffic or computer networks as a form of public protest, they do not typically want to kill, maim, or terrify in the process.[13] The recent successes of hacktivists, however, do highlight the potential threat of cyberterrorism in that a few individuals with little to no moral

restraint may use methods similar to hackers to wreak havoc, generate fear, and cause severe injury or death.[14] The line between cyberterrorism and hacktivism, however, may sometimes blur. This is especially true if terrorist groups are able to recruit or hire computer-savvy hacktivists for their cause or if hacktivists decide to escalate their actions by attacking the systems that operate critical elements of the national infrastructure, such as electric power networks and emergency services.[15]

Security experts have argued for some time that the energy sector has become a potential target for cyber attack through the creation of Internet links—both physical and wireless—that interfere with the supervisory control and data acquisition (SCADA) systems used by electrical and power distribution networks.[16] SCADA systems manage the flow of electricity and natural gas, while also being used to control the industrial systems and facilities used by chemical processing plants, water purification and water delivery operations, wastewater management facilities, and a host of manufacturing firms.[17] Studies have indicated that critical infrastructures that include SCADA systems may be vulnerable to a cyberterrorist attack because the infrastructure and the computer systems used are highly complex, making it effectively impossible to eliminate all potential weaknesses.[18] It is believed by many security professionals that a terrorist's ability to control, disrupt, or alter the command and monitoring functions performed by SCADA systems could threaten regional or national security.[19]

Cyberterrorism, when considered generally, may be conducted by either state or non-state actors, but the calculus and implications can be quite different for each category. Of note, the U.S. Department of State lists three designated state sponsors of terrorism in 2015: Iran, Sudan, and Syria.[20] State sponsored cyberterrorism would most likely be conducted to achieve the goals as defined by the state's political leadership and any actions would tend to support long-term national security goals. Even though the cyber domain offers a bit of anonymity, if a cyber attack is traced back to its network source or Internet address, then the physical location of those perpetrating the attack could be determined within the boundaries of the state authorizing the cyber attack. Because states have geographic boundaries and the initiating computer networks potentially have a physical location, there is increased likelihood, when compared to non-state actors, that those responsible for initiating a state-sponsored cyber attack would be identified.

In contrast, non-state actors—to include many terrorist organizations—do not necessarily act uniformly or according to the same underlying beliefs, and many of the most aggressive organizations are motivated by an ideology that embraces martyrdom and an apocalyptic vision.[21] This ideology may be based on religion or a desire to overthrow a government. Terrorists who are motivated by ideology and intend to conduct cyber attacks against the United States or its interests may not care about the repercussions following an act of cyberterrorism, whether military in scope or not. In

such a scenario, some strategists think a terrorist organization's leadership may prove undeterrable by traditional military means.[22] Despite the disparate motivators of terrorists, many terrorist organizations, to include al-Qaida and the self-proclaimed Islamic State, are said by some security experts to function strategically and rationally.[23] Because a terrorist organization's leadership may be inclined to make rational decisions, deterrence may at times be a suitable method of influencing future actions. Consequently, deterrence should be considered a critical element in a successful national strategy to prevent cyberterrorism.

The Advantages of Cyberterrorism

There are several advantages to using the cyber domain to conduct acts of terrorism. First, cyberterrorism can be far less expensive than traditional terrorist methods.[24] Potentially, all that is needed is a personal computer and an Internet connection, instead of needing to buy weapons, like guns or explosives, or acquire transportation.[25] Second, cyberterrorism has the potential for being more anonymous than traditional, kinetic methods.[26] It can be difficult for security and police agencies to track down the identity of terrorists when they use online "screen names" or are an unidentified "guest user."[27] Third, the number of potential targets is enormous when compared to the number of targets typically used in kinetic actions. The cyberterrorist could target the computer networks of governments, individuals, public utilities, private airlines, SCADA systems, and other critical networks. The sheer number of potential cyber targets is thought to increase the likelihood that an adversary can find a weakness or vulnerability in one of the different networks to exploit. Finally, cyberterrorism can be conducted remotely, a feature that may be especially appealing to some would-be attackers.

Exaggerated Threat?

Many critics have noted, however, that while the potential threat of cyberterrorism is alarming and despite all the dire predictions of impending attack, no single instance of real cyberterrorism has been recorded.[28] To date, there has been no recorded instance of cyberterrorism on U.S. public facilities, transportation systems, nuclear power plants, power grids, or other key components of the national infrastructure. While cyber attacks on critical components of the national infrastructure are not uncommon, such attacks have not been conducted in a manner to cause the kind of damage or severity of effects that would qualify as cyberterrorism.[29] The 2007 widespread denial of service cyber attack in Estonia, which brought down the banking system for three weeks, did not cause catastrophic damage, injury, or death.[30] Even in the case of the Stuxnet malware, discovered in June 2010 and called "world's

first digital weapon" because of its capability of causing physical destruction to computers and other equipment, did not cause widespread, severe destructive effects.[31]

This begs the question: Just how real is the cyberterrorism threat? While cyberterrorism may be an attractive option for modern terrorists who value its remote access, anonymity, potential to inflict massive damage, and psychological impact, some critics say that cyber fears have been exaggerated.[32] Furthermore, there is disagreement among some cyber experts about whether critical infrastructure computers, to include SCADA systems, offer an effective target for furthering terrorists' goals.[33]

Many computer security experts do not believe that it is possible to use the Internet to inflict damage, injury, or death on a large scale.[34] Some of these experts note that critical computer systems are resilient to attack through the investments of time, money, and expertise during the design and development of these critical systems. For example, the U.S. Department of Defense, Central Intelligence Agency, and Federal Bureau of Investigation are reported to protect their most critical systems by isolating —also called air-gapping—them from the Internet and other internal computer networks.[35]

Despite the ongoing debate about whether the cyberterrorism threat is exaggerated or if the potential destructive effects can be sufficiently achieved to warrant concern, both the news media and government reporting indicate that some terrorist organizations now use the Internet to communicate, recruit people, raise funds, and coordinate future attacks.[36] Even though there is no publically available information that terrorist organizations have directly and successfully attacked Internet servers or major computer networks, reporting does suggest that many terrorist organizations would employ cyber means to achieve their goals if the opportunity presented itself.[37] Because there appears to be a persistent desire by some terrorist organizations to use any and all means, including cyber attacks, to achieve their desired goals, it is paramount for policy makers and military planners to take preparatory actions to prevent such acts and mitigate any effects should such an attack occur. These preparatory actions include deterrence efforts.

Deterrence and the Law of Armed Conflict

In a frequently cited definition, deterrence is "persuading a potential enemy that it is in his own interest to avoid certain courses of action."[38] The underlying basis of cyber deterrence theory—a subset of general deterrence—is that credible and potentially overwhelming force or other actions against any would-be adversary is sufficient to deter most potential aggressors from conducting cyber attacks, including those acts considered to be cyberterrorism. When considering deterrence in the cyber domain, it is worth considering the advice of Colin Gray, "given that deterrence can only work, when it does, in the minds of enemy leaders, it is their worldview, not ours, that must

determine whether or not deterrence succeeds."[39] Therefore, to deter a potential adversary, we must deter its leadership or decision makers.

According to deterrence theory, deterrence only works if there is a credible threat of retaliatory action or force. What is considered a credible retaliatory action within the U.S. defense community is typically governed by the Law of Armed Conflict (LOAC), which is sometimes also referred to as the Law of War. While not directive or preventive of any future action, the ideas and principles within the LOAC have relevance when considering any response to terrorism, including those in response to cyberterrorism.

The LOAC has been defined as the part of international law that regulates the conduct of armed hostilities.[40] The LOAC is based on two main sources. The first is customary international law arising out of hostilities and binding on all states, and the second is international treaty law arising from international treaties, which binds only those states that ratified a particular treaty.[41] The purpose of the LOAC is to reduce the damage and casualties of any conflict; protect combatants and noncombatants from unnecessary suffering; safeguard the fundamental rights of combatants and noncombatants; and make it easier to restore peace after the conflict's conclusion.

Two principles contained in the Law of Armed Conflict are most germane to a follow-on act of cyberterrorism, and these are the principles of military necessity and lawful targeting. The first principle, military necessity, calls for using only that degree and kind of force required for the partial or complete submission of the enemy, while considering the minimum expenditure of time, life, and physical resources.[42] This principle is designed to limit the application of force required for carrying out lawful military purposes. Although the principle of military necessity recognizes that some collateral damage and incidental injury to civilians may occur when a legitimate military target is attacked, it does not excuse the destruction of lives and property disproportionate to the military advantage to be gained.[43]

The second principle, lawful targeting, is based on three assumptions: a belligerent's right to injure the enemy is not unlimited; targeting civilian populations for attack is prohibited; and combatants must be distinguished from noncombatants to spare noncombatants injury as much as possible.[44] Consequently, under the principle of lawful targeting, all "reasonable precautions" must be taken to ensure that only military objectives are targeted in order to avoid, as much as possible, damage to civilian objects (collateral damage) and death and injury to civilians (incidental injury).[45]

An offshoot of the concept of deterrence is extended deterrence, which is currently a topic of study and discussion within the U.S. Department of Defense. "Extended deterrence" refers to strengthening regional deterrence and reassuring U.S. allies and partners through the credible threat of retaliatory force.[46] U.S. Strategic Command, which oversees U.S. Cyber Command, recently held a conference to discuss and assess the Defense Department's ability to deter specific state and non-state

actors from conducting cyber attacks of significant consequence on the U.S. homeland and against U.S. interests, to include attacks resulting in loss of life, significant destruction of property, or significant impact on U.S. economic and foreign interests.[47] A topic of the conference also included identifying ways to deter Russia, China, Iran and North Korea from conducting cyber attacks against international allies, which is the realm of extended deterrence.[48] Based upon hundreds of years of treaty precedence, extended deterrence seems to be a viable strategic concept in cyberspace. Article 51, for example, of the Charter of the United Nations acknowledges collective self-defense as an inherent right of one or more states.[49] States being part of an extended deterrence agreement, or collective self-defense treaty, should serve as a means of discouraging conflict or as a means of coming to the defense of allies should deterrence fail. This concept is still relevant in cyberspace.

Suitable Responses to Cyberterrorism

Based upon the principles of military necessity and lawful targeting mentioned previously, a military response to cyberterrorism should only target and attack military objectives. Military objectives are combatants and those objects which, by their nature, location, purpose, or use, effectively contribute to the enemy's war-fighting or war-sustaining capability.[50] They also include objects whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of the attack.[51] Additionally, when considering the cyber-related military objects to target and attack, it is important to understand that it is not unlawful to cause incidental injury to civilians, or collateral damage to civilian objects, during an attack upon a legitimate military objective. Incidental injury or collateral damage must not, however, be excessive in light of the military advantage anticipated by the attack.[52]

Related to the principles within the LOAC, in February 2003, the Bush administration published a report titled *The Strategy to Secure Cyberspace* that stated the U.S. government reserves the right to respond "in an appropriate manner" if the United States comes under computer attack.[53] This response could involve the use of U.S. cyber weapons or malicious code designed to attack and disrupt the targeted computer systems of an adversary.[54] For any follow-on U.S. military actions to be considered "appropriate," these actions would need to be conducted in the spirit of the LOAC.

So, the question to be answered is what specifically is or is not an appropriate response following an act of cyberterrorism? First, taking into account degree and kind of force required for the partial or complete submission of the enemy, any response—whether kinetic or cyber—should not be considered excessive or disproportionate to the military advantage to be gained. Consequently, if the aggressor's

cyber attack caused injury or death to a dozen people, and a resulting cyber counter-attack caused injury or death to a thousand people, with little correlation to a military advantage or gain, then it appears such a situation would not be appropriate within the context of the LOAC. Second, taking into account that a counter-attack to cyberterrorism should target the military objectives contributing to the enemy's war-fighting or war-sustaining capability, then disabling or damaging the adversary's network servers and computer infrastructure, which are routinely used by the aggressor to conduct attacks, would seem to be in agreement with the tenets of the LOAC.

A response to a cyber attack does not need to be military in nature, but may entail nonmilitary actions, such as economic or financial measures. For example, in light of the inordinate and ever growing number of cyber attacks against U.S. systems reaching a threshold to consider a national emergency, President Obama issued an executive order in April 2015, seeking to negatively affect the finances of those behind the attacks. The President's executive order states:

> Starting today, we're giving notice to those who pose significant threats to our security or economy by damaging our critical infrastructure, disrupting or hijacking our computer networks, or stealing the trade secrets of American companies or the personal information of American citizens for profit.[55]

The executive order gives the U.S. Department of Treasury the authority to impose sanctions on individuals or entities responsible for cyber attacks and cyber espionage. In effect, the order allows the freezing of assets when passing through the U.S. financial system and prohibiting those responsible for the cyber attacks from transacting with U.S. companies.

Counterarguments

There are several counterarguments to the contention that deterrence is effective against cyberterrorism. Jim Lewis, for example, has argued that deterrence will not work in the cyber domain.[56] Lewis states that asymmetric vulnerability to attack, new classes of opponents with very different tolerance of risk, and the difficulty of crafting a proportional and credible response all erode the ability to deter in the cyber and space domains.[57] He notes that public and private entities in the United States experience cyber attacks on a daily basis, and if these attacks are deterrable, then the U.S. government is doing a terrible job of leveraging our capabilities.[58]

Other critics argue that the use of cyber weapons in response to an act of cyber aggression could cause effects that are widespread and severe, thereby exceeding the guidance of the LOAC.[59] These resulting effects of cyber weapons may be difficult to limit or control. There is the fear that if a computer software attack is targeted against a terrorist group, then it is possible that the malicious code might inadvertently spread throughout the Internet. This could severely affect or shut down critical infrastructure

systems in other non-combatant countries, including perhaps computers operated by the United States and its allies and partners.

Still other critics say that choosing an actual target for a military response following an act of cyberterrorism instigated by a non-state actor could prove problematic, since non-state sponsored terrorists may not have clear geographic boundaries, making it difficult to avoid affecting civilians. The critical civilian computer systems within the country hosting the terrorist group may be adversely affected by a U.S. cyber attack against the terrorists' computers and network, thereby resulting in effects that are noncompliant with the principle of lawful targeting. This exact problem is why some strategists and policymakers have long argued that deterrence is ineffective against terrorist leadership, since it could appear that a credible response following a cyber attack may not be viable.

Finally, other critics could point out that the United States and other countries would not be bound by the LOAC following a cyber attack by terrorists because terrorists are unlawful combatants who do not follow the LOAC's provisions. After all, unlawful combatants are by definition individuals who directly participate in hostilities without being authorized by a governmental authority, and non-state-sponsored terrorists fall in this category. Nevertheless, any U.S. response to a cyber attack by terrorists—that is, by unlawful combatants—should follow the LOAC's tenets. Indeed, the LOAC addresses terrorist actions specifically by noting that unlawful combatants who engage in hostilities are in violation of the LOAC and in doing so become lawful targets.[60] Consequently, such terrorists may be killed or wounded and, if captured, may be tried as war criminals for their actions.[61]

A Holistic Strategy of Prevention

The goal of a strategy seeking to prevent an act of cyberterrorism is to cause the leadership of an organization to decide that an attack is not worth the cost or that the attack will fail in achieving the desired objectives. As a result, this strategy of prevention should lead these leaders or decision makers not to choose an act of cyberterrorism. While a credible threat of a military response or force is necessary for deterrence to be effective, any means available to achieve this goal of prevention should be considered part of a suitable strategy. Specifically, other means could include nonmilitary activities if they support discouraging a potential adversary from pursuing an act of cyberterrorism. Consequently, an overall strategy of prevention should include both military and nonmilitary approaches that integrate and layer activities. Such a strategy represents a holistic approach for dealing with the threat of cyberterrorism. These military and nonmilitary activities working together to support the goal of prevention can be categorized as *deterrence* and *dissuasion*.

Deterrence

As previously addressed and despite its limitations in affecting the decision-making calculus of a few leaders, deterrence remains a viable concept for discouraging cyberterrorism. Many terrorist organizations, including al-Qaida and the Islamic State, are thought to function strategically and rationally.[62] For this reason, deterrence is still a relevant consideration.

There is nothing within the LOAC that explicitly prohibits a military response to an act of cyberterrorism, even one that is non-state sponsored. As long as the principles of military necessity and lawful targeting are duly considered, both military and nonmilitary responses are viable options.

By conducting persistent and aggressive counterterrorism operations to seek out the most militant terrorist organizations, the United States can increase a potential adversary's perception that there would be a credible threat of force and unacceptable consequence following any attack against the United States. If Islamic State or al-Qaida's leadership believed that following an act of cyberterrorism the United States would systematically seek them through military or nonmilitary means and threaten their survival and power base, they might be deterred from conducting a life threatening cyber attack.

In the case of state-sponsored cyberterrorism, the knowledge that the United States has the option to respond "in an appropriate manner" to a cyber attack may increase the likelihood of deterring states that are involved in cyberterrorism. Therefore, if a hostile state enables terrorists to conduct cyber attacks against the United States or its interests, a U.S. response may include both cyber and non-cyber options. While the problems inherent in selecting a suitable military objective associated with an act of non-state-sponsored terrorism have been noted previously, these problems are mitigated in a scenario involving a supporting or facilitating state, because clear geographic boundaries facilitate taking reasonable precautions to help ensure that collateral damage and incidental injury are avoided as much as possible.

Dissuasion

Besides deterrence, the other part of a holistic strategy is dissuasion, which seeks to influence the leadership of potential adversaries by discouraging the initiation of military competition.[63] To be effective, dissuasion activities must occur before a threat manifests itself. Dissuasion includes "shaping activities," which are typically nonmilitary in scope and conducted during peacetime.[64] Within the lexicon of the U.S. military services, dissuasion is said to work outside the potential threat of military action. A strategy incorporating dissuasion to influence potential cyber adversaries would seek to convey the futility of cyber attacks, thereby causing a potential adversary's leadership not to seek a military confrontation.[65] Worth noting is that some strate-

gists think that those dissuaded from competing with the United States should not need to be deterred.[66] With respect to dissuading those considering cyber attacks, such an approach should focus on three areas: resilience, forensics, and monetary interception.

Resilience efforts, such as those encompassing redundant network hardware and Internet connectivity pathways, hold promise in making a notable improvement in situations following a widespread and potentially devastating cyber attack. Significant preparations that improve cyber resilience and mitigate and manage the consequences following an act of cyberterrorism can cause an adversary's leadership to determine that a cyber attack will not cause the desired destructive effects. Consequently, if an adversary's leadership determines that a cyber attack is unlikely to achieve their objectives, they may refrain from conducting such an attack in the first place, or decide to pursue another path of causing destruction, such as conventional kinetic attacks.

The second aspect of dissuasion is having a reliable and responsive cyber forensics capability. As defined here, cyber forensics is the science of analyzing and determining the origination source and pathway of a cyber attack after such an attack has occurred, for law enforcement or defense counterintelligence purposes. After an act of cyberterrorism, post-attack cyber forensics capabilities will attempt to use any "electronic fingerprints" or other network and software information to facilitate an attribution determination regarding the source and identity of those responsible for launching the cyber attack. Admittedly, identification and follow-on attribution can be difficult tasks because attackers can use computer intermediaries or channel their attack through anonymizing proxies that hide their Internet protocol address.[67] Nonetheless, a robust and publically-known capability to identify and attribute the source of cyber attack could dissuade prospective cyber terrorists or those supporting their efforts. A successful identification and attribution of a cyber attack may lead to prosecution through civilian courts, or for more significant acts of aggression, lead to targeting with kinetic or non-kinetic weapons.

The last area for dissuading cyberterrorism involves aggressive efforts to intercept and minimize the funding streams used by those involved in cyberterrorism. Such intercepting actions may also be called counter threat finance and sanction activities.[68] Funding is acknowledged as being critical to sustaining the activities of many organizations involved in terrorism, to include non-state actors. In the past, such funding to terrorist organizations has come through charities, illegal activities, and front companies. Persistent multinational fiscal interdiction efforts could significantly reduce the funding available to organizations that are most likely to conduct cyberterrorism.

Current U.S. Department of State counter threat finance and sanction activities seek to target those financial transactions benefiting terrorist organizations, whether

coming from states, nongovernmental organizations, or private entities.[69] A sustained effort to eliminate or minimize funding sources used by terrorist organizations could help curtail future recruits for the organization's cause. When combined with cyber resilience and forensics efforts, a terrorist organization's leaders may decide not to seek a direct confrontation through cyberterrorism.

Conclusion

When dissuasion works with deterrence as part of a broad strategy of prevention, there is an increased likelihood of discouraging a potential adversary's leadership from pursuing acts of cyberterrorism. History suggests, however, that deterrence will at times fail due to miscalculation, uncertainty, or chance. This may also be the case for deterring acts of cyberterrorisms. If deterrence fails and an attack occurs, having measures in place to manage the consequences of a widespread and destructive cyber attack could reduce or limit the damage. A side benefit of a strategy incorporating both deterrence and dissuasion concepts is that a broader range of potential state adversaries may be deterred or dissuaded from conducting relatively "routine" or commonplace cyber attacks on the United States or its interests, because it would seem doubtful that the desired effects can be achieved or that such an attack was worth the cost. Perhaps paradoxically, it has been observed that the success in "the 'war on terror' is likely to make terrorists turn increasingly to unconventional weapons such as cyberterrorism."[70] While some terrorism experts have concluded that, at least for now, truck bombs, terrorist financing, and recruitment seem to pose a greater threat than cyberterrorism, the potential cyberterrorism threat cannot be ignored.

Even though an act of cyberterrorism may seem improbable, many considered the 9/11 attacks improbable beforehand as well. Countless ordinary citizens and politicians within the United States regret that more was not done to improve counterterrorism capabilities and strategies before the 9/11 attacks, especially since many of the needed improvements seemed obvious afterwards. Likewise, the time is now to act in implementing a sound and comprehensive strategy to deter and dissuade cyberterrorism, and not after such an attack has occurred.

Notes

1. Office of the Press Secretary, *Fact Sheet: Administration Cybersecurity Efforts 2015*, (Washington, D.C.: The White House, 9 July 2015) https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administrationcybersecurity-efforts-2015.

2. President Barack Obama (remarks, Cybersecurity and Consumer Protection Summit, Stanford University, 13 February 2015), https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-presidentcybersecurity-and-consumer-protection-summit.

3. Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World," *Orbis* 59, no. 1 (2015): 111-128, http://www.sciencedirect.com/science/article/pii/S0030438714000787.

4. Jim Lewis, "The Role of Deterrence," (speech, Space Security Symposium, Stimson Center, 15 November 2012), http://www.stimson.org/about/news/jimlewis-of-csis-speaks-at-stimson-on-cyber-deterrence/.

5. Colin S. Gray, *National Security Dilemmas: Challenges & Opportunities* (Dulles, VA: Potomac Books Inc., 2009), 62.

6. Andrew F. Krepinevich, *Cyber Warfare: A 'Nuclear Option'?* (Washington, DC: Center for Strategic and Budgetary Assessments, 2012), 8, http://csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/.

7. John J. Klein, "Some Principles of Cyber Strategy," *ISN Security Watch*, 21 August 2014, http://www.isn.ethz.ch/DigitalLibrary/Articles/Detail/?id=182955.

8. David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *NYTimes.com*, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-tohacking-against-us.html?pagewanted=all&_r=0.

9. Dorothy Denning, "Cyberterrorism," Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, 23 May 2000, www.stealthiss.com/documents/pdf/cyberterrorism.pdf.

10. Dorothy Denning, "Is Cyber Terror Next?" in *Understanding September*, eds. Craig Calhoun, Paul Price, and Ashley Timmer (New York: The New Press, 2002).

11. Gabriel Weimann, *Cyberterrorism: How Real Is the Threat?* (Washington, D.C.: United States Institute of Peace, December 2004), 4, http://www.usip.org/sites/default/files/sr119.pdf.

12. Ibid.

13. Ibid., 5.

14. Ibid.

15. Ibid.

16. Clay Wilson, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report RJ32114 (Washington, D.C.: Library of Congress, Congressional Research Service, 17 October 2003), 12-13.

17. Keith Stouffer, Joe Falco, and Karen Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security* (Washington, D.C.: U.S. Department of Commerce, 2006), 2-1, http://www.dhs.gov/sites/default/files/publications/csd-nistguidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf.

18. Weimann, *Cyberterrorism*, 6.

19. Ibid., 7.

20. "State Sponsors of Terrorism," Department of State, 2015, http://www.state.gov/j/ct/list/c14151.htm.

21. Keith B. Payne, *How Much is Enough?: A Goal-Driven Approach to Defining Key Principles* (Fairfax, VA: National Institute for Public Policy, 2009), 5.

22. Executive Office of the President, *The National Security Strategy of the United States* (Washington, D.C.: White House, May 2002), 15, http://www.state.gov/documents/organization/63562.pdf.

23. Gray, *National Security Dilemmas*, 72.

24. Weimann, *Cyberterrorism*, 6.

25. In contrast, some experts argue that sophisticated cyber attacks would require greater expense and expertise. See Thomas M. Chen, *Cyberterrorism after Stutxnet* (Carlisle Barracks, PA: United States Army War College Press, June 2014), 22-23, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1211.pdf.

26. Ibid., 10.

27. Weimann, *Cyberterrorism*, 6.

28. Chen, *Cyberterrorism after Stuxnet*, 20.

29. Ibid.

30. Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, http://www.iar-gwu.org/node/65.

31. Dan Holden, "Is Cyber-Terrorism the New Normal," *Wired*, http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/.

32. Weimann, *Cyberterrorism*, 8.

33. Clay, *Computer Attack and Cyber Terrorism*, 12.

34. Weimann, *Cyberterrorism*, 8.

35. Joshua Green, "The Myth of Cyberterrorism," *Washington Monthly* (November 2002), http://www.washingtonmonthly.com/features/2001/0211.green.html.

36. Kenney, "Cyber-Terrorism in a Post-Stuxnet World."

37. Chen, *Cyberterrorism after Stuxnet*, 13.

38. Thomas Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), 9.

39. Gray, *National Security Dilemmas*, 56.

40. U.S. Joint Chiefs of Staff, Joint Publication 1–02, *Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, 8 November 2010), 214, http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf.
41. U.S. Department of the Navy, NWP 1–14M, *The Commander's Handbook on the Law of Naval Operations* (Washington, DC: Department of the Navy, July 2007), 6–5, http://www.lawofwar.org/naval_warfare_publication_N-114M.htm.
42. Ibid.
43. Ibid. This concept is also referred to as the principle of proportionality.
44. Ibid., 8-1.
45. Ibid.
46. This definition is taken from the context of nuclear extended deterrence. See Department of Defense, *Nuclear Posture Review Report* (Washington, D.C.: Department of Defense, April 2010).
47. "U.S. Military Symposium Will Mull Role of 'Extended Deterrence' In Cyberspace," *Inside Defense*, 27 July 2015.
48. Ibid.
49. Article 51, *Charter of the United Nations and Statute of the International Court of Justice* (San Francisco, CA: United Nations, 1945), https://treaties.un.org/doc/publication/ctc/uncharter.pdf.
50. U.S. Department of the Navy, NWP 1–14M, para 8.1.1.
51. Ibid.
52. Ibid., para. 8.1.2.1.
53. Executive Office of the President, *The Strategy to Secure Cyberspace* (Washington, D.C.: White House, 2003), 50, https://www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
54. Clay, *Computer Attack and Cyber Terrorism*, 18-19.
55. Michael Daniel, "Our Latest Tool to Combat Cyber Attacks: What You Need to Know," *The White House (*blog), 1 April 2015, https://www.whitehouse.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attackswhat-you-need-know.
56. Stimson Center, "Jim Lewis of CSIS Speaks at Stimson on Cyber Deterrence," *Stimson.org*, 15 November 2012, http://www.stimson.org/about/news/jim-lewis-of-csis-speaks-at-stimson-on-cyberdeterrence/.
57. Ibid.
58. Ibid.
59. Clay, *Computer Attack and Cyber Terrorism*, 19.
60. International Committee of the Red Cross, "The Relevance of IHL in the Context of Terrorism," (Geneva, Switzerland: ICRC, 1 January 2011).
61. U.S. Department of the Navy, NWP 1–14M, para. 12.7.1.
62. Gray, *National Security Dilemmas*, 72.
63. Department of Defense, *Annual Report to the President and the Congress* (Washington, D.C.: Department of Defense, 2002), 18.
64. Chairman, Joint Chiefs of Staff, *Combating Weapons of Mass Destruction*, JP 3–40 (Washington, D.C.: Department of Defense, 10 June 2009), x.
65. Ibid., I–3.
66. Gray, *National Security Dilemmas*, 59; Denning, "Cyberterrorism."
67. Chen, *Cyberterrorism after Stuxnet*, 4.
68. "Counter Threat Finance and Sanctions," U.S. Department of State, http://www.state.gov/e/eb/tfs/.
69. Ibid.
70. Weimann, *Cyberterrorism*, 11.

Is Cyber Deterrence an Illusory Course of Action?

Emilio Iasiello*

With the U.S. government (USG) acknowledgement of the seriousness of cyber threats, particularly against its critical infrastructures, as well as the Department of Defense (DoD) officially labeling cyberspace as a war fighting domain, security experts, policymakers, and think tank researchers have resurrected a potential Cold War strategy to implement against the new threats fermenting in cyberspace.[1] It is argued that the same principles that successfully contributed to nuclear deterrence with the Soviet Union can be applied to cyberspace and the hostile actors that operate within. However compelling, similar strategies are not transferrable and the key factors that made nuclear deterrence a viable solution do not carry the same value in cyberspace. While only a handful of states have demonstrated the capability to develop nuclear weapons, more than 140 nations have or are developing cyber weapons, and more than thirty countries are creating military cyber units, according to some estimates. Moreover, this threat actor landscape does not consist of nation states alone. Included are cyber criminals, hackers, and hacktivists of varying levels of sophistication and resources willing to use their capabilities to support nefarious objectives.[2]

There are advocates favoring the implementation of a cyber deterrence strategy to mitigate the volume of hostile cyber activity against public and private sector interests. However, too many factors—including attribution challenges and sustainability against this vast threat actor landscape—inhibit cyber deterrence options from achieving their desired outcome in the near term. What's more, other deterrent strategies such as those employed against nuclear weapon use, terrorism, and rogue state behavior are not suitable models for the cyber realm. Despite some commonalities, the cyber domain lacks the transparency and actor visibility required to develop deterrence measures. Despite these hindrances, nation states should seek to develop,

*Emilio Iasiello is the chief threat analyst for a global cyber intelligence firm, supporting federal and commercial entities to manage cyber risks, understand their threat environment, and help prioritize their investments against those threats impacting their business or mission. Emilio has written papers on the development of a new cyber threat analytic methodology, the cyber threat to aviation, a proposal to fix U.S. national cybersecurity efforts, and the IT Supply Chain.

Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?," *Journal of Strategic Security* 7, no. 1 (2013): 54-67. DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5. Available at: http://scholarcommons.usf.edu/jss/vol7/iss1/6.

refine, and implement national level cybersecurity strategies that focus on cyber defense improvements and enforce accountability to measure their successes. While there will always be sophisticated actors able to thwart the most robust cybersecurity defenses, the success of hostile activity against networks are the result of poor cybersecurity practices such as unpatched systems and users not well trained in information assurance principles. Cybersecurity is an ongoing effort that needs to be relentlessly monitored and adapted to a constantly changing threat environment.

What is Cyber Deterrence?

Before one embraces the design and development of a nation state cyber deterrent strategy, it is important to understand the basic concepts of deterrence and what it entails for a strategy of cyber deterrence. At its base, a deterrence strategy seeks to influence an adversary from not attacking a target by making him believe the costs and consequences will outweigh any potential benefits. Therefore, a working definition by the author and perhaps more importantly what it involves and its intended effects may sound something like this:

> Cyber deterrence is a strategy by which a defending state seeks to maintain the status quo by signaling its intentions to deter hostile cyber activity by targeting and influencing an adversary's decision making apparatus to avoid engaging in destructive cyber activity for fear of a greater reprisal by the initial aggressor.

With this baseline understanding, it is equally essential to identify the types of deterrence that are available and have been used throughout the course of history. Although there are a myriad of iterations and subsets, there are largely two types of deterrence strategies employed by the United States—deterrence by punishment and deterrence by denial.

- **Deterrence by punishment** intimates to an attacker that there will be significant punishment in retaliation for an attack.[3] In this scenario, retaliation need not be limited to specific actions, but can incorporate other means as well, such as kinetic strikes or more diplomatic means such as economic sanctions.[4] An example of deterrence by punishment is the Cold War's mutually assured destruction doctrine wherein the threat of using a nuclear weapon prevented an adversary from using a similar weapon.

  Applying the same principle to cyberspace, deterrence by punishment can take the form of digital actions such as a retaliatory cyber strike against perpetrators of a cyber attack, or a pre-emptive strike against adversaries mounting an attack against networks. However, deterrence by punishment against a cyber attack could also entail kinetic attacks against targets, diplomatic bargaining, or economic sanctions. If one believes that the United States

was behind the STUXNET attack that targeted Iranian nuclear centrifuges, this could be perceived as a pre-emptive deterrence by punishment against Iran for continuing to refine its uranium enrichment procedures.

- **Deterrence by denial** is less conflict driven, seeking to convince potential attackers that their effort will not succeed and they will be denied the benefits they seek.[5] The benefit of this strategy is that it may be based on defensive measures and thus not only be a means of preventing the enemy from acting but also providing a solution in case the challenger decides to act.[6] An example of this type of deterrence is the U.S. naval blockade around Cuba in 1962. In this instance, the United States opted to deny entry to Russian ships from entering Cuban waters rather than deploying air strikes against Cuban missile sites.

  In cyberspace, deterrence by denial assumes a more traditional defensive role by discouraging or frustrating attacks via robust, proactive, and costly defenses. It requires a large, focused commitment by the government to secure the systems and networks under its control, in tandem with the full cooperation of the private owners of the infrastructure.[7] The cost increases significantly given the breadth of this endeavor including the use of advanced security practices and the adoption of trusted hardware and software components.[8]

Necessary Factors for Effective Cyber Deterrence

Cyber deterrence is difficult to execute, as there are several factors that must occur in order to achieve the results of either subset of deterrence strategy. A cyber deterrence strategy must have established parameters from which to operate successfully. Without them, an adversary will not be able to receive and process the defender's intent, which runs the risks of misunderstanding or misinterpreting them, thereby increasing the risk of escalation and quite possibly, that of state on state confrontation.

Communication

Part of any deterrence strategy is to be able to effectively communicate to the international community, and particularly adversaries, on what is acceptable and what are redlines that will be addressed if crossed. In *Arms and Influence*, author Thomas Schelling notes that successful deterrence using either punishment or denial methods depends upon effective communication between a state and the entity it wishes to deter.[9] Working in tandem with communication is the notion of credibility. A nation state must not just pronounce activity it considers to cross redlines, but must be prepared to act as a result of that activity. A nation state risks losing its international credibility when it fails to do this. An example of this occurred in 2012 when President Barack Obama proclaimed that any use of chemical weapons by the Syrian

government against its citizenry would result in a crossed redline.[10] However, once intelligence confirmed that chemical weapons had been used six months later, Obama still had not acted to back up his public assertion.[11] By refusing to back up his bold statement, the United States lost some of its credibility. Even after it agreed to supply the Syrian rebels with arms in July 2013, many in the international community viewed this as "too little too late."[12]

In cyberspace, communication assumes an important function given that the domain is one steeped in ambiguity. Effective communication would require a consensus for operating norms of behavior in cyberspace, a difficult endeavor to achieve as evidenced when the United States and China failed to identify common language in the July 2013 Strategic and Economic Dialogue.[13] The United States prefers to use the term "cybersecurity" to focus on the technologies and networks of automated machines, whereas countries like China and Russia prefer to use the broader term "information security" to include the information resident on or passing through networks as well as the technologies themselves.[14] The key to this discrepancy rests in the activities that occur in cyberspace; China is pursuing a broader interpretation to be able to dictate and control the content and information to which its citizenry has access, whereas the U.S. supports the policy of Internet freedom. As of the second December 2013 meeting of the China–U.S. Cybersecurity Working Group, the two countries remain at an impasse in finding common ground on definition language. Without a common lexicon in place, communication between the two sides is fated to remain in disagreement, failing to achieve consensus on how the Internet should be used appropriately. Similarly, when addressing hostile activities in cyberspace where the actors are foreign to each other, the inability to communicate further impedes the ability to send clear messages and deescalate tensions. The 2001 Council of Europe led Convention on Cybercrime provides a good framework from which agreed upon terminology can be achieved. The agreement successfully identifies key terminology agreed upon by all signatories. To date, there have been forty-one ratifications/accessions to the Convention. Notably, while listed as a non-member state, Russia has yet to sign or ratify the agreement, and China has not joined indicating their reluctance to accept terminology agreed to by Western States.[15]

Signaling

Signaling game logic has been applied to many areas of international politics in the past decade, including decisions to go to war, crisis bargaining, international economic negotiations, regional integration, and foreign policies of democratic states.[16] Whether in peacetime or war, a key element of any cyber deterrence strategy includes the ability to properly signal intentions to the receiver. Without the ability to signal, cyber deterrence by punishment is rendered ineffective and runs the risk of being misunderstood or misinterpreted, increasing the risk of escalation and conflict. For

example, prior to the execution of deterrence by punishment, the defending state must clearly signal its discontent to the aggressor (whether a nation state or non-state actor) in such a way that the aggressor interprets it correctly, understands it, and concludes that the potential costs of undertaking such action far outweigh any potential benefits. However, it should be noted that the signaling nation state must have an established body of work and credibility conducting successful and destructive cyber retaliation for signaling to be effective. If the adversary does not believe the credibility of a signaling nation state or if it flat out does not care, it is immaterial how much signaling is completed. In this case, the aggressor will not be deterred by threat of punishment.

Like communication, signaling in cyberspace can be easily misinterpreted, ignored, or not even noticed by the aggressor. Signaling can be done overtly, covertly, or through diplomatic, economic, or military channels. Take for example the STUXNET incident. If the United States government were responsible for the deployment of STUXNET on Iranian centrifuges, the USG may have signaled to the Iranian government through diplomatic channels that such an action—without revealing the intended target—would transpire if Iran did not cease its enrichment process. Thus, when the centrifuges broke down and were replaced, it would have been clear that the United States was behind the event. Another example of potential signaling in cyberspace would be the use of distributed denial-of-service (DDoS) attacks. Continuing with the STUXNET scenario, U.S. banks were targeted by DDoS attacks shortly after the discovery of STUXNET. Many U.S. lawmakers immediately suspected the Iranian government to having conducted or orchestrated the attacks via proxies.[17] If Iran was responsible, prior signaling through diplomatic or third party channels without revealing specific targets would have clearly conveyed to the USG that Iran was not only responding to the STUXNET attack, but also that it had a cyber capability to do so as well.

Attribution

It is extremely difficult to determine attribution in cyberspace where savvy operators have a multitude of obfuscation techniques to thwart defenders from correctly identifying their true point of origin. Whether it's compromising a series of computers in different countries prior to executing attacks, or using anonymizers and proxies, cyberspace is an environment favoring those seeking to conduct surreptitious malicious acts. Attribution is a necessary component of any deterrence strategy as it is incumbent on the defending state to positively attribute an aggressor prior to the commencement of any retaliatory action. However, complete attribution may not be needed to engage in deterrence by denial where other forms of non-destructive actions can be directed against an aggressor. Jason Healey of the Atlantic Council presents a strong case for determining the "spectrum of state responsibility," a tool de-

signed to help analysts with imperfect knowledge assign responsibility for a particular attack, or a campaign of attacks, with more precision and transparency.[18] The spectrum assigns ten categories, each marked by a different degree of responsibility, based on whether a nation ignores, abets, or conducts an attack.[19] The level of attributed nation state culpability would serve as the guide for the type and appropriate level of response ranging from ignoring the initial attack or striking back at the perceived aggressor.

Successful attribution practices in cyberspace will ideally meld technical, cognitive, and behavioral analysis to better identify the aggressors, as well as those influences that may be helping to guide their operations. Technical analysis is not sufficient for attribution purposes, considering many hostile actors implement the same tactics, techniques, and procedures, as well as tools, or engage in "false flag" operations in conducting malicious activity.[20] No standard exists today for establishing a degree of confidence in determining cyber attribution.[21] When it comes to possibly deploying a cyber deterrence by punishment, the defender must be able to identify the perpetrator for an appropriate response action. Several problems inhibit quick and accurate attribution processes including: misattribution; the time it takes to collect and analyze the attack method employed; and identifying actor motive, behavior, and outside influences. Nevertheless, in order to avoid public embarrassment and reduce the volume and likelihood of collateral damage, an acceptable level of attribution must be performed prior to the commencement of any retaliatory action.

Proportionality

Based on the 1949 Geneva Conventions on the Law of Armed Conflict and the principles of proportionality, as well as those expressed in NATO's recent drafting of the Tallinn Manual advocating cyber war's assimilation into conventional warfare, a retaliatory cyber action needs to be proportional, particularly if leveled against a suspected state or state-sponsored actor. That is, "it must be comparable to the initial wrong and not equate to an escalation."[22] Here, a nation state's credibility is interlinked with proportionality in that the nation state must not only strike back against the aggressor but it must do so in a way as to make its point—that is, it must be a forceful strike—but not so forceful as to solicit negative reaction in the global community. A nation state's credibility on the world stage rests in its ability to back what it says, and be judicious enough not to be perceived as heavy-handed. What is more, it needs to consider unintended consequences as a result of cyber retaliation. Take for example the STUXNET worm used against Iranian nuclear centrifuges. The malware was written to target specific configuration requirements, in this case, the Siemens software resident on the centrifuges.

However, despite being surreptitiously inserted and deployed on a non-Internet connected network, the virus did escape, infecting computers in Azerbaijan, Indone-

sia, India, Pakistan, and the United States.[23] Such outcomes can not only prove detrimental to a nation state's public image, but also risk bringing in third party nation states or politically or ideologically motivated actors into the conflict (e.g., the hacker attacks against U.S. government websites after the accidental bombing of the Chinese Embassy in the then Yugoslavia in 1999 and the initiation of the 2001 China–U.S. hacker conflict after the collision of a U.S. spy plane and a Chinese jet).[24]

Proportionality in cyberspace is difficult to achieve for a variety of reasons. It should reflect the commensurate amount of damage done to a target that was suffered by the victim as to mitigate the risk of escalation. Perhaps more importantly, when a nation state acts independently of a respected international organization such as the United Nations mandate, it runs the risk of diplomatic and even economic blowback for its action. Therefore, prior to retaliation, the type of kinetic or non-kinetic response, the promptness of the retaliation, the projected consequences and battle damage assessment, and the potential political fallout should all be factored in the decision-making process.

Other Deterrence Strategies

There are other deterrent strategies that have achieved mixed levels of success that can be used as potential benchmarks for cyber deterrence. In these cases, while there are some shared commonalities such as diverse threat actor landscapes, asymmetric capabilities of defenders and aggressors, and military operations, each have their own unique challenges that can't be assimilated to the cyber environment. A brief examination of nuclear, terrorism, and rogue state deterrence models will serve as comparative paradigms to see if some of the principles that make them successful can be applied to the cyber domain.

Nuclear Deterrence

There is no greater example of a successful deterrent strategy than that demonstrated by the United States and the Soviet Union during the Cold War. At its core, nuclear deterrence was directed at states already armed with nuclear weapons and was aimed at deterring their use.[25] By the early 1970s, the "mutually assured destruction" theory prevailed; neither the United States nor the Soviet Union was motivated, foolish, ignorant, or incoherent enough to accept the risk of nuclear war.[26] The results of nuclear deterrence have been a resounding achievement, as no nation state since that time has ever deployed a nuclear weapon against a target, as the costs in lives, recovery, international prestige, and natural resources have far outweighed any prospective benefit to using nuclear weapons in any conflict.

But can the principles involved in nuclear deterrence be applied to cyberspace? Widely viewed as an asymmetric power/threat like its nuclear counterpart, the cyber

domain is easily translatable into a similar paradigm in certain areas. Below are key similarities shared between cyber and nuclear deterrence strategies:

Key Similarities between Cyber and Nuclear Conflict:

1. Both operate at all three levels of military operations: strategic, operational, and tactical, with the potential to have effects ranging from small- to population-scale.
2. Both have the capacity to create large-scale, even existentially, destructive effects.
3. Both can be conducted between nation-states, between a nation-state and non-state actors, or between hybrids involving nation-states and non-state actor proxies.
4. Both nuclear and cyber conflict "could present the adversary with decisive defeat, negating the need to fight conventional wars."
5. Both can intentionally or unintentionally cause *cascade effects* beyond the scope of the original attack target.[27]

However, despite some crossover, there are too many inconsistencies that prevent an even partial adoption of the nuclear deterrence model. These range from the volume of actors operating in cyberspace to the comparison of weapon strength to the dual use nature of the tools themselves.

Key differences include:

1. Nation states typically do not assume responsibility for hostile actions taken in cyberspace.
2. There has been no awe inspiring, game changing show of what a cyber attack can do; while incidents like STUXNET and the wiper malware that destroyed 30,000 hard drives for the Saudi oil company Saudi Aramco were significant disruptions, they were not enough to severely impact operations at either the nuclear facility or the oil company.
3. Attribution in cyberspace is extremely difficult and cannot be as precise as identifying a nation state that has launched a nuclear weapon and,
4. Unlike nuclear weapons development, which can be monitored, there is no similar transparency for nation state production of cyber weapons, nor an international watchdog agency to track such developments.[28]

Factor in the involvement of proxy groups and third party cutouts, the expanding and borderless nature of the operating environment, and the uncertainty that actors can actually be deterred, and it is evident that the same fundamental transparencies that have made nuclear deterrence a success do not have the same applicability in cyberspace.

Terrorism Deterrence

Several authors believe that terrorism deterrence can succeed on some level, particularly if a terrorist organization assumes the attributes of a nation state, when real assets can be damaged influencing terrorist leadership to constrain its policies in order to preserve them.[29] One author argues that the assassination of top-level leaders and operational commanders have had a temporary deterrent effect, if only to provide a lull time in which these groups have had to reorganize themselves.[30] Another author advocates for deterrence to achieve success against the terrorist target, the threatened party must understand the (implicit or explicit) threat, and decision-making by the adversary must be sufficiently influenced by calculations of costs and benefits.[31] Another author states that even if terrorists are generally not deterrable some specific terrorist actions may be deterrable even today.[32]

Nevertheless, there are far more obstacles to, rather than benefits from, deterring terrorism, many of which are shared by the cyber domain, particularly when it comes to trying to deter a perseverant adversary that does not necessarily reside in one or the same location. How does one deter the activities of an individual or group without knowing who they are or where they reside?

Another factor complicating deterrence efforts is motivation. While the terrorist leadership may value their own lives, groups are full of individuals willing to die for a cause. United Kingdom national security scholar John Gearson suggests that traditional concepts of deterrence will not work against a terrorist enemy whose avowed tactics are wanton destruction and the targeting of innocents; whose so called soldiers seek martyrdom and death and whose most potent protection is statelessness.[33] Upon closer inspection, the first half of Gearson's statement is very applicable toward hostile cyber actors as well. Actors motivated by a cause, whether political, ideological, or financial, are hard pressed to be deterred unless some formative action can cause them significant physical, emotional, or financial impact to curb engagement in further hostile activity in cyberspace.

Another facet challenging a successful deterrence strategy is consistently influencing terrorist behavior. In order to be successful, a direct response deterrent threat must be made conditional on an adversary's behavior; if individuals and political groups believe that they will be targeted as part of the U.S. war on terror regardless of their actions, they have less incentive to show restraint.[34] To date, there have been no publicly observed incidents or evidence where cyber deterrence by denial or punishment has been successfully used to mitigate hostile cyber activity, or influence the actors directing or conducting the activity.

Rogue States

The United States also engages in deterrent strategies against those rogue states that pose a threat to its national security interests. There are cases to be made on both sides of the equation regarding if U.S. policies successfully deter states such as Syria and North Korea. On one hand, there has not been a military conflict between the United States and these adversaries suggesting current deterrence efforts have been a success. On the other hand, these states continue to pursue programs viewed by the U.S. government as hostile regardless of U.S. diplomatic/economic efforts to halt their progress. In its second term, the Bush administration announced a new approach that it called "tailored deterrence" to be leveraged against these rogue states.[35] The basis for this line of reasoning was that different strategies could be crafted for different states and situations, and that the United States would have to learn what regimes valued most in order to develop a deterrent strategy that would most effectively target the psychological profiles of their leaders.[36] However, there are recent anecdotal examples that illustrate why rogue state deterrence is difficult to achieve.

- **North Korea**: In 2013, North Korea conducted its third nuclear test. In response, the United States sent B-52 bombers followed by B-2 stealth bombers on practice flights over South Korea. North Korea responded by increased hostile rhetoric and appeared prepared to launch a test flight of a new missile. Worried about escalating the situation, the U.S. dialed back its comments and military maneuvers.[37] In this instance, deterrent military actions did not reduce tensions between the U.S. and North Korea, and even risked escalating matters to a military conflict.
- **Syria**: In August 2012, in response to Syrian rebels attempting to overthrow the Syrian regime of Bashar al-Assad, President Barack Obama stated that any use of chemical weapons would cross a "red line." The President bolstered these comments in December adding that use of chemical weapons would have "consequences"—bureaucratic-speak for potential kinetic or military responses.[38] However, when the United States failed to act once chemical weapons had been used, the U.S. government lost considerable credibility—a necessary component of a deterrent by punishment strategy.

Potential removal from office is not always a deterrent factor when dealing with rogue nation states run by authoritarian regimes. What is more, the removal of leaders still has not dissuaded other totalitarian leaders from their courses of action. For example, Muammar Gaddafi's besiegement by civil war in 2011 coupled with his ultimate demise with the support of U.S. and material and logistical support has done nothing to convince Syria's al-Assad to step down.

Similarly, nation state operators, mercenary groups for hire, hacktivists, or criminals will likely be undeterred by law enforcement, intelligence, or military engage-

ment. Cyber criminals continue their activities despite several high profile international arrests.[39] Suspected nation state actors continue to engage in cyber espionage despite being called out in public forums.[40]

Operation Ababil hacktivists continue to conduct DDoS attacks against U.S. financial institutions for the better part of a year and a half without consequence.[41] Ultimately, trying to apply a rogue state deterrent strategy against the cyber environment may not be a suitable fit, due to the complexity and diversity of the threat actor landscape. Many of these actors do not operate like a rogue state whose ultimate purpose is regime stability and preservation of leadership; as such, these actors do not cherish the same values. Even suspected nation state actors answer to their chain of command and would only stop given the proper instruction from above.

Can Cyber Deterrence Work?

Martin Libicki states that the goal of cyber deterrence is to reduce "the risk of cyberattacks to an acceptable level at an acceptable cost," where the defending nation state mitigates potential offensive action by threatening a potent retaliation.[42] But can such a policy actually be successful? While it is entirely possible that cyber deterrence will not be executed in a vacuum, in its 2011 *Strategy for Operating in Cyberspace*, the DoD justified the use of active cyber defense measures to prevent intrusions and affect adversary activities on DoD networks and systems.[43] This responsibility, coupled with the disclosure of the once classified "Presidential Policy Directive-20" (if this is a legitimate document), indicate that the U.S. can engage in offensive cyber activity to curb an imminent threat, or ongoing attacks that do not require prior Presidential approval, suggesting that deterrent cyber actions may be conducted as an isolated effort.[44] Therefore, taken in this context, prior to engaging in a retaliatory strike back option, it is necessary to make some points clear with regards to cyber deterrence. In no way does advocating offensive actions for defensive purposes nullify the need to have an established cyber defense posture. As such, some truths remain:

1. **Traditional Cyber Defenses Still Need to Be in Place.** An argument can be made that a successful "deterrence by punishment" policy would greatly reduce expenditures associated with traditional cybersecurity to include devices, programs, and the costs associated with upkeep, maintenance, and replacement. However, this is misleading. A deterrence strategy cannot address all of cyberspace's hostile actors. If deterrence is meant to dissuade serious actors such as nation states or the more sophisticated cyber criminals and hacktivists groups, what will stop the majority of other "noise" that targets networks? Jim Lewis, a cyber expert from the Center of Strategic & International Studies, states that "survey data consistently shows that 80-90 percent of successful breaches of corporate networks required only the most basic techniques, and that 96 percent of those could have been

avoided if proper security controls were in place."[45] Indeed, the same sentiment was expressed when Australia's Defense Signals Directorate in partnership with the U.S. National Security Agency came up with a list of measures that would mitigate most of the "successful" attacks they had surveyed in 2009 and 2010.[46] Thus, even the most basic computer security practices would still be required in order to achieve maximum cyber defense coverage.

2. **Deterrence by Punishment Relies on the Rationality of Actors**. Deterrence is an option that will work only if the people/groups/government being deterred are rational; and as such, can be deterred because they are unwilling to risk losing something of greater value. Currently, adversaries operate in cyberspace because they do not fear retaliation due to known attribution challenges, and the connected, nebulous, unsecure environment favors their maneuvers. Therefore, a nation state may be more conducive to deterrence than a terrorist or hacktivist organization. If the adversary does not hold a rational view of the world and his place in it, or he does not have anything to lose or be threatened, he may be very difficult to deter from a specific course of action.

3. **The Adversary Must Have Something of Value**. Building on the previous statement, the adversary must have something of value for a pre-emptive/retaliatory strike to be effective. If he doesn't, then the threat of cyber deterrence becomes inconsequential. For example, a nation state likely has many assets linked to the Internet or are at least networked. But what if it is a closed state? For example, North Korea has very few online assets connected to the Internet that can be targeted remotely (suggesting that any effective cyber operation against a high value target would have to be conducted via close operations, as was suspected in the STUXNET incident). And if the adversary is a cellular-structured terrorist or hacktivist group dispersed globally, what value point can be leveraged that will have sway over the actions of the entire group?

With these truths in mind, and upon review of current deterrence strategies against other targets, it is evident that cyber deterrence by punishment success rests in three fundamental axioms:

- **Attribution**. It may seem like common sense, but it is essential for a government to know who attacked it before launching any counterattack. But how does one gain reasonable confidence in a domain that thrives on ambiguity? There are so many factors to consider prior to launching a retaliatory strike including but not limited to: the attacker's identity (If linked to a nation state, did the attacker receive orders from above or is he acting alone? If a third party, is it working on behalf of a nation state government or just acting to support it? Is it a false flag operation, why or why not?); motivations for the attack (What prompted the attack? Was it in itself retaliation for something that the

targeted nation state did?); and the intention of the attack (Was the intent of the attack to destroy, degrade, deny, or disrupt, or something else? Did the attack have an intended purpose other than what is being seen on the surface?). Also, some things to consider: if the originating attack were viewed as cause-motivated, several states, hackers, or hacktivists would have reasons for having conducted the attack. Even if these third parties were acting on behalf of the state, do you hold the state or the actors responsible? Who exactly is the target —the nation state pulling the strings or the actors conducting the attacks?

But is attribution enough? When one looks at the amount of governments that have singled out China as the main hacking threat to their nations, little has been done to either stop or deter Chinese cyber espionage. President Obama has had several talks with Chinese counterpart Xi Jinping that has yet to yield any substantive results.[47] While there has been no known U.S. attempt at conducting a retaliatory strike (as of yet) against the Chinese, this goes to prove that attribution is not a panacea, even when directly confronting the alleged perpetrator directly, and that the challenge remains to convince the attacker that he has in fact been caught doing something specific.[48]

- **Repeatability**. Repeatability across many different threat actors is an important facet of cyber deterrence, and one of its biggest questions. Can individual actors, cyber criminal groups, foreign intelligence services, military units all be deterred using the same strategy? A quick answer is no. Different strategies and applications would have to be applied to different actor targets. For example, how a government might deter a criminal group targeting its defense industrial base may be different than how it might deter an adversarial nation state, or even an allied one, from conducting espionage activity. For many large, well-networked nation states, the cyber threat actors targeting its assets are diverse. Suffice to say, individual actors and smaller, less capable groups (unless working on behalf of an adversarial nation state) are unlikely to be on the end of a retaliatory cyber attack for their activities. However, larger, more sophisticated cyber crime groups, hacktivists, and nation state actors are more primed for retaliation as they generally generate more publicity and cause the most damage. For deterrence by punishment to work effectively, the target needs to understand that the retaliatory action is a direct result of the offending action. If a target fails to understand the retaliation, it may be necessary to repeat the act using stronger, more obvious tactics. However, this runs the risk of misinterpretation by the target, and if the target has failed to understand the retaliatory nature of the cyber attack, it may see such an attack as an originating act. This could quickly escalate the situation into greater cyber conflict.

- **Success**. In the case of cyber deterrence by punishment, there is the tactical objective of either stopping a cyber attack while it's happening, punishing the offenders after it happened, or punishing the offenders prior to them launching an initial attack. In the case of punishing an offender during a cyber attack, the objective would be to get him to stop attacking; in the case of punishing an offender after attack, the objective would be to hurt him so he will not engage in similar activity in the future; and finally, in the case of a preemptive strike, the objective would be to again hurt him enough so that he will be deterred from ever engaging in an attack. Tactically, these objectives all have merit, but how will they strategically be viable? In other words, would the battle be won at the expense of losing the war? For example, engaging in a pre-emptive or retaliatory cyber strike presupposes that you have successfully attributed, identified, and reconnoitered the target, presumably, in this case, the computer from which the adversary is operating. While the pre-emptive/retaliatory strike may destroy that computer, the adversary may have ten or fifty more computers from which to keep operating. In this example, can the defending nation believe that they really won the engagement? In another example, if the pre-emptive/retaliatory strike is directed at a different target (e.g., a power grid, a critical infrastructure, etc.), how does the victim state take proportionality into account, especially if the adversary has not even conducted an attack? Furthermore, how does the defending state know that the adversary will understand that the pre-emptive/retaliatory strike is in response to potential, ongoing, or future action, and that the message of deterrence will be received, and accepted? What is more, if the adversary is a nation state, how does one account for potential escalatory actions as a result of a perceived disproportionate retaliatory strike? Martin Libicki points out that:

> attackers are likely to escalate if they (1) do not believe cyber retaliation is merited; (2) face internal pressures to respond in an obviously painful way; or (3) believe they will lose in a cyber tit-for-tat but can counter in domains where they enjoy superiority.[49]

Conclusion

In cyberspace, the effort to counter hostile acts through use of preemptive or retaliatory strikes may seem like a step in the right direction, especially when considering the failures suffered by defenders to mitigate the threat of malicious activity. However, thousands of cyber attacks occur per day, suggesting great difficulty in distinguishing serious threats from minor ones.[50] Stepping on an ant in your kitchen doesn't prevent an infestation; similarly, cyber deterrence is not a panacea for threat

actors seeking to exploit public and private sector networks. At present, there are too many unexplored variables and an undeveloped plan for its use to make this an effective course of action.

Attribution challenges, the ability to respond quickly, effectively, and accurately, and the ability to create and sustain a model by which repeatability can be leveraged against different threat actors will continue to prove too insurmountable in the near term for victimized countries to launch pre-emptive or retaliatory cyber strikes. Cyber deterrence by denial has a better chance of succeeding; however, only in a limited capacity as network defenders have consistently been beaten by smarter, more agile adversaries obfuscating themselves in cyberspace. Instead of striking back against adversaries, organizations need to evaluate their current security postures to determine its effectiveness in the current cyber climate.

Cybersecurity is not a static solution; as attackers gain more knowledge and experience, their tactics, techniques, and procedures will morph over time. Defense strategies that worked a year ago will likely not have the same success given the rate at which this landscape changes. According to the Department of Homeland Security's U.S. Computer Emergency Response Team,

> a comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems along with processes to be informed of current threats and enable timely response and recovery.[51]

Organizations need to implement adaptable security plans that take into account the dynamic aspects of cyberspace, and include milestones and performance measures to ensure that goals are met in a timely manner. Stricter security standards such as vulnerability patching and user awareness must be enacted in order to hold stakeholders accountable for compliance failure. The well-respected SANS Institute, a leader in computer security training and certification, advocates the implementation of twenty security controls for cyber defense, and maintains that organizations successfully incorporating these controls have reduced their security risk.[52] Ultimately, due diligence with respect to cybersecurity is the deciding factor in combating hostile cyber activity.

Notes

1. The White House. *International Strategy for Cyberspace*, Washington, DC, May 2011; Department of Defense. *Department of Defense's Strategy for Operating in Cyberspace*, Washington, DC, July 2011, http://www.defense.gov/news/d20110714cyber.pdf.

2. "Nuclear Weapons: Who Has Them At a Glance | Arms Control Association," April 2013, http://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat; Susan W. Brenner and Leo L. Clarke, "Civilians in Cyberwarfare: Casualties," *SMU Science & Technology Law Review* 13 (2010): 249; Graham H. Todd, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition," *Air Force Law Review* 64, rev 96 (2009); William J. Lynn III, "The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack," *Foreign Affairs* (28 September 2011), www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later.

3. Jeffrey W. Knopf, "Use with Caution: The Value and Limits of Deterrence Against Asymmetric Threats," *World Politics Review* (11 June 2013), http://www.worldpoliticsreview.com/articles/13006/use-with-cautionthe-value-and-limits-of-deterrence-against-asymmetric-threats.

4. Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," *Military and Strategic Affairs* 3, no. 3 (December 2011): 54.

5. Knopf, "Use with Caution."

6. Lupovici, "Cyber Warfare and Deterrence," 54.

7. David Elliott, "Deterring Strategic Cyberattack," *IEEE Security & Privacy* 9, no. 5 (September/October 2011): 36-40.

8. W.K. Clark and P.L. Levin, "Securing the Information Highway," *Foreign* Affairs, (November/December 2009): 2-10.

9. Jonathan Solomon, "Cyberdeterrence between Nation States: Plausible Strategy or Pipe Dream?," *Strategic Studies Quarterly* 5, no. 1 (2011): 2.

10. "Obama Warns Al-Asad Against Chemical Weapons, Declares 'World is Watching,'" *CNN Online*, 3 December 2012, http://www.cnn.com/2012/12/03/world/meast/syria-civil-war.

11. Terrence Burlij and Christina Bellantoni, "Syria Crossed Obama's Redline. What Happens Next?" *PBS Online*, 14 June 2013, http://www.pbs.org/newshour/rundown/2013/06/administration-sharpens-focus-onsyria-with-chemical-weapons-report.html.

12. "Few Satisfied, But U.S. Presses Syrian Arms Effort," *Las Vegas Sun Online*, 26 July 2013, http://www.lasvegassun.com/news/2013/jul/26/us-obama-aid-to-syria/.

13. Bill Gertz, "U.S., China Strategic and Economic Dialogue Criticized," *Washington Free Beacon*, 16 July 2013, http://freebeacon.com/u-s-china-conclude-strategic-and-economic-dialogue-talks/.

14. "China and Russia Submit Cyber Proposal | Arms Control Association," November 2011, http://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal.

15. "Convention on Cybercrime," *Council of Europe*, CETS No. 185, 25 November 2013, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.

16. James Igoe Walsh, "Do States Play Signaling Games?" *Cooperation and Conflict: Journal of the Nordic International Studies Association* 42, no. 4 (2007): 441.

17. Ellen Nakashima, "Iran Blamed for Cyberattacks on U.S. Banks and Companies," *The Washington Post*, 21 September 2012, http://articles.washingtonpost.com/2012-09-21/world/35497878_1_web-sitesquds-force-cyberattacks.

18. Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," *Atlantic Council*, January 2012, http://www.acus.org/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF.

19. Ibid.

20. Kelly Jackson Higgins, "The Intersection Between Cyberespionage and Cybercrime," *Dark Reading*, 21 June 2012, http://www.darkreading.com/attacks-breaches/the-intersection-betweencyberespionage/240002514; Kelly Jackson Higgins, "Attackers Engage in False Flag Attack Manipulation," *Dark Reading*, 1 October 2012, http://www.darkreading.com/attacks-breaches/attackers-engage-in-falseflag-attack-ma/240008256.

21. Emilio Iasiello, "Identifying Cyber-Attackers to Require High-Tech Sleuthing Skills," *National Defense*, December 2012, http://www.nationaldefensemagazine.org/archive/2012/December/Pages/IdentifyingCyber-AttackerstoRequireHigh-TechSleuthingSkills.aspx.

22. Eric Talbon Jensen, "Cyber Deterrence," *Emory International Law Review* 26, no. 2 (2012): 799.

23. "W32.Stuxnet," *Symantec*, 26 February 2013, http://www.symantec.com/security_response/writeup.isp?docid=2010-071400-3123-99.

24. Ellen Mesmer, "Kosovo Cyber War Intensifies; Chinese Hackers Targeting U.S. Sites, Government Says," *CNN Online*, 12 May 1999, http://www.cnn.com/TECH/computing/9905/12/cyberwar.idg/; Craig S. Smith, "May 6-12: The First World Hacker War," *The New York Times*, 13 May 2001, http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html.

25. Jeffrey Record, "Nuclear Deterrence, Preventative War, and Counterproliferation," *The Cato Institute* 519 (8 July 2004), http://www.cato.org/sites/cato.org/files/pubs/pdf/pa519.pdf.

26. Keith B. Payne and C. Dale Walton, "Deterrence in the Post-Cold War World," *Strategy in the Contemporary World, An Introduction to Strategic Studies*, ed. John Baylis, James Wirtz, Eliot Cohen, and Gray Colins, (New York: Oxford University Press, 2002), 169.

27. James C. Mulvenon and Gregory J. Rattray, "Addressing Cyber Instability: Executive Summary," *The Atlantic Council*, 8 July 2004, http://www.acus.org/files/CCSA_Addressing_Cyber_Instability.pdf.

28. Iasiello, Emilio, *Cyber Attack: A Dull Tool to Shape Foreign Policy* (Tallinn: NATO CCD COE Publications, May 2013), 398.

29. Shmuel Bar, "Deterring Terrorists," *Hoover Institution*, 2 June 2008, http://www.hoover.org/publications/policy-review/article/5674.

30. Ibid.

31. Robert F. Trager and Dessislava P. Zagorcheva, "Deterring Terrorism," *International Security* 30 no. 3 (Winter 2005/2006): 87.

32. Paul K. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda* (Santa Monica, CA: RAND Corp., 2002), 59.

33. John Gearson, "Deterring Conventional Terrorism: From Punishment to Denial and Resilience," *Contemporary Security Policy* 33, no. 1 (2012): 171.

34. Matt Kroenig and Barry Pavel, "How to Deter Terrorism," *The Washington Quarterly* 5, no. 2 (Spring 2012): 21.

35. Knopf, "Use With Caution."

36. Ibid.

37. Ibid.

38. Ibid.

39. "FBI: More Arrests in International Cyber Crime Takedown," *Infosec Island*, 13 July 2012, http://www.infosecisland.com/blogview/21907-FBI-More-Arrests-in-International-Cyber-Crime-Takedown.html; James O'Toole, "Global Financial Cybercrime Sting Yields 24 Arrests," *Money CNN Online*, 26 June 2012, http://money.cnn.com/2012/06/26/technology/cybercrime-arrests/index.htm.

40. Steve Ragan, "China's APT 1 Still Operating with the Same Modus Operandi," *Security Week*, 1 May 2013, http://www.securityweek.com/chinas-apt1-still-operating-same-modus-operandi.

41. Tracy Kitten, "DDoS: Attackers Announce Phase 4," *Bank Info Security*, 23 July 2013, http://www.bankinfosecurity.com/ddos-attackers-announce-phase-4-a-5929/op-1.

42. Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corp., 2009), http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

43. Department of Defense. *Strategy for Operating in Cyberspace*, Washington, DC: Department of Defense, June 2011, http://www.defense.gov/news/d20110714cyber.pdf.

44. "Obama Tells Intelligence Chiefs to Draw up Cyber Target List – Full Document Text," *The Guardian*, 7 June 2013, http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text.

45. James A. Lewis, "Raising the Bar on Cyber Security," *Center for Strategic & International Studies*, (12 February 2013), http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf.

46. Ibid.

47. Scott Neumann, "Chinese Cyber Hacking Discussed at Obama-Xi Summit," *NPR Online*, 9 June 2013, http://www.npr.org/blogs/thetwo-way/2013/06/09/190058558/chinese-cyber-hacking-discussed-at-obama-xisummit; Lucian Constantin, "The Chinese Hacker Group that Hit the New York Times is Back with Updated Tools," *Computerworld*, 12 August 2013, http://www.computerworld.com/s/article/9241577/The_Chinese_hacker_group_that_hit_the_N.Y._Times_is_back_with_updated_tools.

48. Libicki, *Cyberdeterrence and Cyberwar*.

49. Ibid.

50. Franklin D. Kramer, "Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Books, Inc. and National Defense University Press, 2009), 15.

51. Eric Byers, "Essential Cyber Security Concepts for CEOs," *Belden*, 28 February 2013, http://www.belden.com/blog/industrialsecurity/Essential-Cyber-Security-Concepts-for-CEOs.cfm.

52. "SANS Institute – CIS Critical Security Controls," http://www.sans.org/critical-security-controls/.

Sharia as 'Desert Business'

Understanding the Links between Criminal Networks and Jihadism in Northern Mali

Rikke Haugegaard*

Despite efforts by the UN peacekeeping mission, the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA), French forces and neighbor states, the security situation in Mali remains fragile. In 2015 and 2016, militant jihadists increased attacks on government forces, humanitarians and UN peacekeepers.[1] Up to 31 March 2017, the MINUSMA mission had 116 fatalities. The majority of the fatalities are from Chad, Burkina Faso, Niger, Togo and Guinea.[2] Militant jihadists, often categorized as 'terrorists' by the international community and staff in MINUSMA, conduct many of these attacks.

The label 'terrorists' covers militant groups using terrorist methods. They all promote Sharia and strict Islamic rule, but their motivations are not linked to religious fanaticism. The jihadist militant groups are driven by a combination of local ambitions for power, internal clan disputes, economic interests in the smuggling business and regional power struggles.[3] During my field visits to MINUSMA, I experienced how MINUSMA personnel were struggling to understand the internal dynamics of the jihadist militant groups and their constant fragmentation.[4] This article contributes to the ongoing discussion on how to understand the complex dynamics between jihadist groups, crime and politics in the Gao and Kidal regions.[5]

The field study in MINUSMA led me to the following research question: How can we understand the social and economic dynamics that enable the operative space of the militant networks in northern Mali? The argument proposed here is to move away from analyzing jihadist militant groups as organizations and 'closed' entities. Rather, they are loose networks of supporters, mobilized for contextual violent attacks. The focus here is to investigate the jihadist militant groups as products of local

*Lecturer and analyst at Royal Danish Defence College, Denmark. Ms. Haugegaard is affiliated with the Section for Military Operational Culture at the Danish Defence Language Institute where she supports and develops culture training and education for a wide range of clients within the Danish Defence as well as international partners.

Rikke Haugegaard, "Sharia as 'Desert Business': Understanding the Links between Criminal Networks and Jihadism in Northern Mali," *Stability: International Journal of Security and Development* 6, no. 1 (2017), 4. DOI: http://doi.org/10.5334/sta.494.

power struggles and involvement in trade and crime rather than as fighters with ideological and religious motivations. Understanding these dynamics will expand the context for framing the militant groups in Mali and beyond.

The sharp distinctions drawn by the Malian government and the international community between compliant and non-compliant groups in the implementation of the peace agreement are problematic. It leaves certain groups out and undermines the possibility of creating a solution to decades of conflict. Dividing actors into these categories (compliant versus non-compliant) impedes MINUSMA's long-term stabilization effort, since lived reality is much more fluid, ad hoc and complex. The complexity of the network mechanisms and the pragmatic shift in alliances represent a challenge for MINUSMA. Military planners and analysts tend to focus on detailed information about the enemy, at the expense of understanding the political, economic and cultural environment that supports 'the enemy.'[6]

The argument develops around a nuanced cultural perspective encompassing the fluidity of social networks. There is an urgent need to turn away from the 'enemy-focused' approach.[7] The concepts 'bigmanity'[8] and 'shadow networks'[9] will be used to discuss the fragmentation of armed groups and the overlap of criminal and political networks in Mali. The author's field data pointed to an important and ongoing challenge for the MINUSMA staff: how to understand the dynamics of the jihadist militant groups in Mali. In the field study (see next section on methodology), the research focus was to review analytical practice in MINUSMA for cracks and analytical challenges. Subsequently, this article is a discussion paper, which questions some of the basic assumptions in the work of MINUSMA staff and the wider international community of consultants, advisors, military and analysts working on the peace process in Mali.

The article starts with reflections on methodology, followed by an introduction to some of the challenges to the ongoing peace process. After a discussion of the label 'terrorist armed group,' the article then moves on to a section on the concept of 'bigmanity,'[10] which can help the analysis of complex social dynamics in northern Mali. Later, the role of AQIM (Al-Qaeda in the Islamic Maghreb) is discussed. The article then provides sections on economic interests and Sharia as 'desert business', looking at the relationship between formal and informal network structures. Finally, the article concludes with a short discussion on local conflicts in northern Mali, leading to a closing with reflections on implications for the peace process in Mali.

Reflections on methodology

This article is based on my personal field experience:

- conducting fieldwork in MINUSMA in November 2014 and October 2015. In total, spending 23 days in MINUSMA, working with military officers, analysts and civil advisors;
- attending briefings, meetings and patrols;
- conducting 34 interviews. The selection criteria were nationality, age, gender, and research topic/task and mission experience;
- accessing MINUSMA through the Danish Defence and the respective Commanders of the All Source Information Fusion Unit (ASIFU);[11]
- working as a guest researcher in MINUSMA, trying to follow the daily working procedures of the staff as closely as possible;
- wearing a military uniform to 'blend in';
- sleeping in tents and containers in the MINUSMA camps in Bamako and Gao;
- attending briefings and meetings, reading reports, visiting MINUSMA HQ and conducting a few patrols together with military personnel in Bamako and Gao;
- working for the Danish Defense as a researcher and lecturer for more than five years, prior to this field study.

The process of enculturation into military thinking can lead to biases, where daily processes and certain analytical models are taken for granted. However, as a cultural anthropologist, critical thinking about state institutions and power relations is vital. This article challenges the basic assumptions among MINUSMA staff: that some militant groups can be labeled as 'terrorists' and therefore non-compliant in the peace agreement. In addition, can we understand these entities as 'groups' with well-defined members and the structure of an organization?

Challenges to the peace process

"Implementation will prove challenging in a country where there is a history of agreements not being implemented."

—Arthur Boutellis[12]

Implementing the peace agreement in Mali is challenged by three main factors: lack of jobs opportunities, the presence of armed groups and the exclusion from the peace agreement of armed groups labeled terrorists. The fragile security situation is one of the UN's many challenges. Mali is ranked among the ten poorest countries on the UNDP Human Development Index.[13] The prices of basic food supplies are higher in Gao, Timbuktu and Kidal than in the rest of the country.[14] The UN reached an important milestone in its stability efforts when "The Agreement on Peace and Rec-

onciliation in Mali" was adopted on 20 June 2015.[15] Facilitated by an international mediation team, the two major umbrella organizations, "Platform" and "Coordination", agreed to participate in a process of disarmament and demobilization. "Platform" is a coalition of pro-government militias, supporting a unified Mali. "Coordination" is an alliance of several militant groups fighting for self-government for the Azawad region in northern Mali and neighboring countries. In addition, the two alliances agreed on the release of prisoners and reopening of schools. "Platform" and "Coordination" are considered compliant parties in the peace agreement process, whereas the UN and the Malian government consider militant groups labeled as terrorist organizations non-compliant.

The lack of job opportunities for the combatants in the north complicates the demobilization effort. The tourism industry in Mali used to be thriving, employing ethnic Tuaregs as tour operators, guides and drivers.[16] Both in Mali and Niger, the tourism sector is controlled by the Tuaregs.[17] The tourism industry has collapsed due to the kidnapping threat to western tourists,[18] which means that the Tuaregs' job and food security is now threatened. In addition, there is a food crisis in the northern and eastern regions: 294,000 persons in Mali were expected to be in need of emergency food assistance in 2016, and more than 50 per cent of them live in the northern and eastern regions of Mopti, Timbuktu, Gao and Kidal.[19] Opportunities to work as a teacher are also limited due to lack of open schools. In many smaller towns in the north, schools have been closed due to violent clashes between "Coordination," "Platform" and other militant groups taking over the schools. The UN reports 20 cases of military use of schools, including schools occupied by compliant groups taking part in the peace process.[20] A second important challenge to the implementation of the peace agreement is the mobility of armed groups. Armed groups fight over control of smuggling routes. The groups block roads and secure that drugs, weapons and other goods can pass through the desert areas. Some staff in MINUSMA describes it as 'naval warfare in the desert'. Armed groups fight over important nodes and 'harbors' where smuggled goods are loaded and prepared for further transport through the Sahel. The armed groups are very mobile and move around freely in the open desert areas. Occasionally, they work together on attacks or help each other with logistics. The armed groups cross the borders to neighboring countries unchecked and have networks and contacts in the wider Sahel region. AQIM and affiliated groups take advantage of the Sahelian states' inability to control borders and the peripheral territory.[21]

The third important challenge is the 'terrorist armed groups' excluded from the agreement. Mali hosts both regional Al-Qaeda-affiliated groups, who recruit their members across borders in the whole of the Sahel region (northern Mali, Mauritania, Niger, Burkina Faso and Algeria), and a locally-based group, Ansar Dine, run by Tuaregs from northern Mali.[22] The largest group, AQIM, is striving to become a federation of terror groups in the region but its leadership consists mainly of mem-

bers from Algeria.[23] In 2012, when the jihadist groups controlled the three northern cities of Timbuktu, Gao and Kidal, they tried to establish 'emirates' based on Sharia. Laws against music, movies, smoking and alcohol were enforced through Koran-endorsed punishments such as amputation, lashing or stoning.[24]

Terrorist armed groups–a problematic term

With more than 13,000 soldiers, police and civilian staff deployed in Mali, the UN presence on the ground may at first glance seem rather large. However, scrutiny reveals that the desert areas in the north lack both soldiers and police because many countries contributing to MINUSMA are reluctant to deploy their personnel in the areas where militant armed groups are present. In October 2014, then MINUSMA Force Commander Kazura briefed the UN Security Council on the challenges facing MINUSMA. Kazura stated that "MINUSMA is in a terrorist-fighting situation without an anti-terrorist mandate or adequate training, equipment, logistics or intelligence to deal with such a situation."[25] However, MINUSMA is not mandated to engage in explicit counterterrorism tasks;[26] these tasks are assigned to the Malian government and the French forces present in the Sahel. Despite the presence of the French and Malian forces in the north, jihadists can easily hide in the open desert areas in the northern regions. With a long-term strategy of immersion in local communities and the regional economy, AQIM is developing resilience against counter-terror efforts.[27] Modibo Goïta explains that one of the major problems is that the governments of Mali and Mauritania rely on conventional military means to respond to the jihadists' small and highly mobile units.[28] In addition, AQIM tactically "use the desert as its fallback base."[29] Olivier Guitta mentions three major reasons why AQIM has chosen to build a base in northern Mali, "First, it is a very inhospitable area with difficult terrain making it tough for nations to monitor it, even for U.S. satellites. Second, some Arab tribes are located there and finally, the Malian regime is weak."[30]

The Arab tribes, mainly the Fulani people, control many business networks in northern Mali and are well connected through family networks in neighboring countries.[31] It is important for the jihadists that the local infrastructure is suitable for their business of violent attacks and smuggling. Despite the clear signs of jihadist presence in northern Mali, we should be cautious about categorizing the conflicts in the region as terrorism. According to Morten Bøås, it is problematic to frame the conflicts as a "war on terror;"[32] It is therefore clearly a danger that what is essentially a local conflict in Kidal and northern Mali may be locked in a "war on terror" framework, in which the accusation of Al-Qaeda connections becomes a self-fulfilling prophecy as local insurgencies have nowhere else to turn. This is particularly dangerous as connections already exist on a pragmatic business level, but thus far there is no firm or

widespread ideological attachment. Bøås warns against isolating the armed groups linked to Al-Qaeda. People in northern Mali are well connected through daily life, smuggling and business activities. The field data from a study conducted by Peter Tinti shows similar findings of working relations between traffickers and militants, "who were narco-traffickers first, ideologues second, if at all."[33]

The population in Mali is a landscape of people who position themselves in networks and operate through a palette of possible alliances. The jihadist terrorist groups are very pragmatic and sensitive to the local cultural context[34] and the pragmatism shown by jihadist networks is important. An example is from Gao in 2012, where residents demonstrated against the banning of television, video games and soccer. The jihadists changed course and lifted the ban and even started to buy televisions for several youth organizations.[35] The way people pragmatically operate and position themselves according to funding possibilities points to a complex dynamic between jihadism and negotiations for peace. For this reason, it makes sense to question the distinction between the "compliant" and the "non-compliant" actors in the peace process in Mali. The fragmentation of armed groups and the fluid identities of members regularly crossing the line between "compliant" and "non-compliant" groups demand a different approach.

As one MINUSMA officer pointed out, "everybody knows everybody in Mali. People are well connected."[36] People are indeed linked to each other through large and loose networks and they are easily mobilized for different purposes such as criminal activities and local politics. A study of the network connections between Islamists and rebels in Mali[37] reveals that efficient terrorist networks should avoid being decentralized in too many cells.[38] In Mali, networks composed of both Islamists and rebels (non-compliant and compliant groups, author's note added) can be reached through relatively few intermediaries.[39] This point tells us that non-compliant and compliant groups can work together in practice but some groups (Ansar Dine, AQIM and Al Murabitoun) are excluded from the negotiations on the peace process. A related question is how one should understand the militant jihadists. As one MINUSMA staff explained: "Whether we should call them 'combatants' or 'fighters' is a difficult question. I think what we see in the northern parts of Mali is actually that people are 'active supporters' or a 'reserve force.'"[40] It is very much about the context of the situation, and also about networks, whether a certain militant leader can mobilize people to fight in combat. The quote was a key inspiration for this article. Why do the majority of MINUSMA's staff continue to discuss different militant actors as well-established organizations/groups (as I witnessed in briefings and documents during the field study in 2014 and 2015)? The interesting question is whether the success of the jihadist militants can be explained by their ability to activate a loose network of supporters, a network mobilized by key individuals.

Buying influence and loyalty in Kidal– Big Men and people as infrastructure

"Kidal is a very special place. A town of warriors where people fight over identity. This is the town where Tuareg culture meets Arab culture,"[41] said a Danish military linguist when asked to describe the north-eastern city Kidal. Bøås explains that the Tuareg rebellions are related to internal clan politics in Kidal and disputes over smuggling routes and suggests that in Kidal, "it is the very ability to combine politics and crime, the legal and the illicit and the formal and the informal, which characterizes a successful Big Man in this area."[42] In the introduction to his book (of which Bøås' article is part), Mats Utas describes big men and their networks[43]. According to the anthropologist Marshall Sahlins, "the indicative quality of big-man authority is everywhere the same: it is personal power."[44] The Big Man is able to attract followers based on his ability to assist people privately.[45] Building power "is based on amassing wealth and redistributing it with 'astutely calculated generosity.'"[46] When we study areas like northern Mali, where big men are in power, it is possible to "see people themselves as infrastructure."[47] In other words, people use other people for their own purposes. People maneuver in society through other people's networks, which is why connectivity is vital. People establish links to several big men with competing interests because they want to be able to extract wealth from many different sources. Bigmanity forms loose social webs based on reciprocity. The Big Man earns loyalty and support from his followers, and the followers enjoy what the Big Man provides: economic possibilities, protection and social security.[48]

When I visited MINUSMA in 2014, staff working in Gao stated that local network dynamics are really difficult to grasp: "'friends' and 'enemies' are tangled up in northern Mali, and people can change identity according to their own interests."[49] Again, the concept of bigmanity seems relevant when analyzing why people distribute their loyalty:

> If the Big Man does not distribute enough largesse, he will eventually lose his supporters. Bigmanity is unfixed and multiple. Bigmanity is not a matter of inherited patron-client structures, but rather fluid and ever-changeable webs of relations. [...] Followers may discard Big Men when they do not deliver. At the same time, a follower is not loyal to just one Big Man, but typically enjoys different relationships with different Big Men.[50]

Big men and bricolage– fragmentation dynamics of jihadist militant groups

Bøås argues that violence in northern Mali is pragmatic and ad hoc by nature.[51] Violence pops up occasionally; it is perceived as an opportunity. Pragmatic and ad

hoc alliances are formed around violent action to control trading/smuggling points or achieve political goals or economic gains. As seen in other parts of West Africa, conflicts can occur without ideology and ethnicity being the main drivers. Young fighters join armed groups as their way of "social navigation."[52] They fight for future opportunities and to achieve the important status of being "adult" in society. Young men in Guinea-Bissau, where Henrik Vigh did his research, experience a daily struggle to survive socially. In the cities, the hardship of unemployment makes it an experience of "social death"—the "absence of the possibility of a worthy life."[53] In the northern regions of Mali, where unemployment, droughts and social stagnation are rampant, jihadist armed groups can easily recruit from the pool of dissatisfied young men seeking status, money and power. There is also a general tendency towards youths becoming militarized, due to the drug culture and widespread presence of small arms in the region.[54]

In an analysis of the Tuareg movement in Niger, the *Mouvement des Nigériens pour la Justice* (MNJ), the Tuareg rebellion is characterized by circumstantial alliances, shifting loyalties and a "'hop on–hop off' rebellion loosely controlled by chiefs."[55] The same dynamics are seen in Mali, and these pragmatic and ad hoc alliances have several consequences for the peace process. The landscape of militant groups constantly changes; new groups are formed and other groups dissolve. "Armed groups in Mali are not static groups with stable hierarchies, but more loose groupings constantly fragmenting and adjusting themselves to the strategic situation."[56] Members of "non-compliant" groups like Ansar Dine and MUJAO have left these groups and joined "compliant" groups like HCUA (High Council for the Unity of Azawad, member of the Coalition) and MAA-Sidi Mohamed (member of the "Platform" alliance).[57] Another example of a shift in identity, or of playing different alliances, is the former MUJAO Islamic police chief in Gao, Yoro Ould Daha (who served as police chief during the occupation of Gao in 2012). Today, Daha is commander for the 'Platform' alliance.[58] During my field study in Mali in 2015, I observed many interesting discussions between MINUSMA staff on how to understand the formation of jihadist armed groups and their frequent fragmentation. In this article, I analyse the jihadist armed groups and their splinter groups through the lens of bigmanity.[59] How is it then possible to explain the constant shift between groups and the formation of new armed groups? Yvan Guichaoua suggests using the concept of "bricolage" for the fragile tactics of the rebel Tuaregs.[60] "Bricolage" is a sort of handiwork or "do-it-yourself project." If armed groups really work as "do-it-yourself-projects," this could explain the way groups fragment quite often, because rebel leaders want their "own" project. The fragmentation can be seen as linked to the economic motivation of becoming a Big Man in the smuggling industry, being able to invest in the villages and establish a high-status reputation locally. The fragmentation dynamics of the armed

groups can be analyzed as a phenomenon urging fighters to splinter out of a desire to earn money and become their own "bricoleur."

In his discussions on how to counter insurgents, David Kilcullen explains that modern insurgents "often employ diffuse, cell-based structures and 'leaderless resistance.'"[61] The insurgents are often wealthier than the population.[62] This is also the case in Mali, so trying to isolate the jihadist militant groups will not work well, since the jihadists often invest in local trade and sponsor food and health services. In recent years, jihadist groups have acted as social security providers, fulfilling important roles for the northern population by providing medical and food aid, schooling, financial donations and fuel.[63] The jihadist groups are thus providing social security in places where the Malian government has failed to deliver for decades. Despite the ability to act as organizations, "modern insurgents operate more like a self-synchronizing swarm of independent, but cooperating cells, than like a formal organization."[64] Overall strategic goals and ideology are less important to the jihadist groups. Jihadist militant groups in Mali act as loose frameworks for a range of different "bricolage" activities. If violence in northern Mali is a "hop on – hop off" campaign of smuggling and fighting, it changes our perceptions of loyalty and network dynamics. If we consider the armed groups in Mali as loose groupings, ad hoc and pragmatic in their nature,[65] how does the fragmentation of groups influence the long term peace process? One possible answer, as discussed above, could be that people use each other as infrastructure and position themselves in different networks around big men.[66] The dynamics of bigmanity is the first factor that influences the fragmentation of groups. In northern Mali, we see loose groupings constantly fragmenting.[67] Groups dissolve and new groups are formed around a "Big Man wannabe." MINUSMA must take these dynamics into account when negotiating with actors in the peace process. New groups will be formed, and their members will shift their loyalties to achieve the most in ongoing power struggles.

Understanding bigmanity is crucial for understanding the complexity of the social, economic and political dynamics in northern Mali. The bigmanity concept provides us with an understanding of how people operate in different networks and use each other as infrastructure.[68] The concept of bigmanity also explains how jihadists from Algeria, Malian security officials and other people with resources can establish a bigmanity-type relation to local citizens in northern Mali. The predecessor organization to AQIM, the GSPC,[69] operating in northern Mali in an effort to win hearts and minds, is a good example of how local alliances are formed. The GSPC distributed antibiotics, bought goats and married women from different clans; these alliances lasted only as long as money was flowing to the locals.[70] A prominent Big Man in Mali is Iyad Ag Ghaly, and his influence and ability to mobilize networks will be discussed in the next section.

The role of AQIM

Tuareg communities did not previously engage with groups like AQIM. Today, several community leaders claim that "declining economic opportunities are driving some 'into the arms of AQIM.'"[71] In recent years, AQIM and affiliated jihadist groups have been exacerbating the economic situation in the Sahel through low-level terrorist attacks and criminal activities.[72] Guitta argues that AQIM uses this strategy deliberately to destroy the tourism industry and sabotage foreign investment in the region.[73] As Anderson argues, the label terrorist is a simplified categorical opposition of Good and Evil.[74] Terrorists are supposed to be driven by fanaticism and operate outside norms of war and peace;[75] however, the terrorists in northern Mali are driven by economic and political motivations rather than strict religious fanaticism. Findings indicate that AQIM have shifted their strategy from strict implementation of Sharia and regular punishment to a long-term influence campaign targeted at local populations. This strategy involves creating jobs in remote areas, marrying locals to develop lasting relations and reinvesting ransoms in the local economy.[76] Economic incentives are important for recruitment and AQIM established business partnerships with local elites in order to act as service providers.[77] A comparative study conducted by Caitriona Dowd in Kenya, Mali and Nigeria shows how "grievances regarding economic and political exclusion are typically higher than average in areas subsequently affected by Islamist violence" and perceptions of marginalization are thriving in communities affected by Islamist violence.[78]

An important element of the AQIM strategy also involves influencing key leaders in northern Mali and gaining popular support by publicizing negative statements about the Malian and Mauritanian government.[79] The group Ansar Dine is a good example of why "terrorist armed group" is a problematic term. Iyad Ag Ghali, a former soldier in Gaddafi's army and later a diplomat for the Malian government, formed the group in 2011. The group is considered a "terrorist armed group" by MINUSMA. Ag Ghali was subject to dialogue with and influence from jihadist ideology from AQIM and Pakistani preachers in Mali for decades before he decided to form the group in 2011.[80] Did Ag Ghali later swear allegiance to Al-Qaeda because he was ideologically motivated to engage in jihad? Or was it a result of the election where Ag Ghali failed to be appointed as the next Amenokal (clan head) among the Ifoghas in Kidal? The answer is not clear but Ag Ghali is a key figure in understanding how networks are interconnected in Mali. Ag Ghali is a key broker between Islamist/jihadist networks and rebel networks fighting for independence in northern Mali. Studies of networks in Mali show that Ag Ghali is extremely well connected to other players in Mali, due to his past working as a diplomat and negotiator for the government of Mali.[81] Ag Ghali also tried to become leader of the secular movement MNLA but was defeated because people perceived him as the main creator of previous unpopular peace agreements.[82] Ag Ghali's close relation to the Malian govern-

ment was one of the reasons he had become a discredited figure among the Tuaregs. Vying for power but excluded from tribal or rebel commands, he set himself up as a religious figure.[83] If local conflicts matter—which this article argues—it is worth paying attention to how violence is connected to crime and to local power struggles.

If Bøås is right in claiming that violence is conducted by ad hoc alliances formed by people who already know each other,[84] it might be useful to look at the relation between trade and violence. Smuggling is the main trade in northern Mali and I discussed the link between smuggling and violence with an officer, who worked for MINUSMA in 2014. He confirmed that MINUSMA staff was interested in possible connections between smuggling routes in and through Mali and incidents of violent clashes between armed groups.[85] Data collected by MINUSMA showed that violent clashes often take place in areas where smugglers are fighting over access to routes and smuggling junctions. Therefore, the economic interests and motivations driving the conflicts will be investigated in the next section.

Economic interests and motivations– sources of income for militant groups

The sources of income for militant groups extend beyond kidnappings. According to the UN, the groups generate income by raiding/stealing and taxing goods illegally. In some regions, there are signs of close co-operation between drug smugglers and jihadist networks like AQIM.[86] It is estimated that the strongest group present in Mali, Al-Qaeda in Maghreb (AQIM), has accumulated close to USD 65 million from ransoms from kidnappings conducted by themselves or by criminal groups who pass the hostages on to AQIM.[87] The estimated USD 65 million incomes were calculated in 2013 and the 2016 figure is probably higher. Despite lack of evidence to prove it, Malians generally believe that the hostage negotiators, who work to secure the release of the hostages, take a portion of the ransom and share it with Mali government officials.[88] A local militant leader argues that European states are financing the militant groups: "It is the Western countries that are financing terrorism and jihad through their ransom payments."[89] Malian government officials are reportedly involved in drug trafficking and the facilitation of other criminal activities.[90] Criminal networks are linked to government officials in a complex web of people and transactions. According to Carolyn Nordstrom, we need to look at the relationship between formal and informal structures in society.[91] In war-torn societies, we may find very powerful "shadow networks" with a vast influence on how power and wealth are distributed. It is often impossible to make clear distinctions between legal and illegal, state and non-state, local and international.[92]

Organized crime is one of the root causes of the current conflicts in Mali but it also functions as an opportunity to combat poverty and unemployment. Organized

crime is closely linked to national and local politics as local criminals try to buy political influence through donations and food packages to villages; some even run for local or national elections.[93] Nordstrom is relevant to the analysis of jihadist militant groups in northern Mali because she argues that we should look at how individual key players are involved across what are normally seen as either formal or informal structures. Politics and crime are inter-connected in Mali. Local power brokers capitalize on legal networks to enhance their criminal activities because networks overlap.[94] Businessmen, politicians, military officers, police and local leaders are all involved in the smuggling of weapons, cocaine, cigarettes and human beings.[95] Throughout the Sahelian region, AQIM has established "direct collusive associations with government and security officials. […] As a result, AQIM can not only more ably confront and resist government security services but also undermine Sahelian states from within."[96] The following section will show why smuggling is vital for jihadist armed groups.

Sharia as "desert business"

Smuggling of drugs and weapons is a growing business in West Africa. The smuggling of drugs starts at sea or through air transport from South America. In West Africa, the drugs are loaded onto land transport in three regional areas, Mali and the south-eastern part of Mauritania being two of the key locations.[97] Infiltration by the international drug cartels, smugglers and criminals in sections of the security forces is a threat to many West African states. This infiltration has weakened customs and border controls.[98] In Mali, where criminals infiltrate and operate through governmental structures, this is very much the case. The smuggling business is driven by networks of local politicians and criminals in cooperation with militant jihadists, who operate swiftly and easily in desert areas. Smugglers also use schoolchildren as drug carriers.[99]

The relation between criminals and jihadist militants is one of common interests. The "ordinary" criminals, the smugglers, help the jihadists by buying weapons, ammunition and equipment. In return, militant jihadists facilitate free passage for smuggled goods and trafficking of people through the areas they control. The advantage for AQIM and other jihadists involved in this exchange relationship is that the smugglers help provide weapons and equipment, thus allowing a group like AQIM to avoid exposing itself.[100] According to Francesco Strazzari, AQIM will typically use portions of the profit from ransoms to invest in the drugs traffickers' network.[101] The militant groups labeled as "terrorists" can be seen to act as local security providers and investors. Their substantial investments in the smuggling networks help the smugglers expand their business. The smuggling networks in turn act as logistical support elements for jihadist militants like AQIM and related groups, buying goods and food

at the local markets for the jihadists, who can hide from MINUSMA's presence in the city centers. The business relation between criminals and jihadist militant groups is another reason why the distinction between "compliant" and "non-compliant" groups in the peace process can be questioned. According to Boutellis, when members and financers of jihadist groups and networks shift to "compliant" groups, they continue their business of smuggling and trafficking.[102] Boutellis suggests that a tacit understanding of supporting each other exists between criminal armed groups, the local population and extremist groups.[103] However, this understanding can take the form of the extremist groups threatening citizens and criminals to co-operate.[104]

In northern Mali, the implementation of Sharia is very much about creating space for the smuggling industry. In 2012–2013,

> Arab based movements preached the ideology of borderless jihadism, claiming that custom duties and tariffs are illicit under Sharia law. In Timbuktu, local jihadi movements (i.e. AQIM and allies) reportedly tried to conquer the hearts and minds of local residents by launching an impressive campaign in favor of traders, traffickers and smugglers, explicitly stating that custom duties, tolls, tariffs and frontiers would no longer be enforced.[105]

Strazzari's data from field interviews in 2013 supports the argument presented here that jihadism is closely intertwined with smuggling and trafficking activities. In the desert areas of northern Mali, Sharia is not primarily an ideology; Sharia is a certain way of doing "desert business." An example is the former leading figure in AQIM, Mokhtar Belmokhtar, who founded his network and personal fortune on the smuggling of cigarettes.[106] The pragmatism of jihadist militant groups is closely related to their economic interests.[107] Hence, in the northern regions of Mali, it seems difficult to distinguish between crime, politics and jihadism. Rather, militant networks are involved in a continuum of various activities in a crime-politics-jihadism nexus.

Kidal as contested space

According to Bøås, the conflict in northern Mali is an internal Kidal affair.[108] Other sources support his point of view that Kidal played an important role as a base for traffickers, which was critical in the 2006–2007 Tuareg rebellion, and control over drug routes was crucial in the fighting.[109] The enhanced competition among armed groups over resources and the protection of drug routes fueled the conflict in 2012.[110] Another prominent voice in understanding political violence in Africa, Caitriona Dowd, argues that "Islamist violence emerges in sub-national contexts shaped by governance practices of political and economic marginalization."[111] Events in northern Mali in May 2014 support Dowd's argument. On 17 May 2014, Malian Prime Minister, Moussa Mara travelled to Kidal and was attacked by armed groups. Six civil servants died in the incident.[112] The Malian government considered this attack a

"declaration of war" and responded four days later by launching an attack on Kidal. The result was 30 casualties among Malian government forces. The governmental forces sought refuge at MINUSMA camps in Kidal and other cities in the north.[113] This situation changed the power balance radically. At the end of May 2015, the armed movements MNLA, HCUA and others were now in control and started to set up a parallel administration, including local security committees.[114] The attack by the Malian security forces paved the way for a disintegration of the governmental structure in the north. It also left MINUSMA with the dilemma of how to work with militant groups, who are now the de facto authorities in Kidal.[115] In February 2016, jihadist militant groups attacked the MINUSMA camp in Kidal, killing five MINUSMA peacekeepers and wounding 30 staff members. Since then, efforts have been made by MINUSMA to arrange meetings in Kidal—the "Forum in Kidal"—between local actors and the Malian government. However, the Malian government seems reluctant to participate and finds it unacceptable to visit Kidal when the government is not hosting the meeting. "We should not be invited to an event on our own soil," said Malian foreign minister Abdoulaye Diop when commenting on the "Forum in Kidal" and the status of the peace process in Mali.[116]

As stated earlier in this article, years of marginalization and ignorance have fueled the conflict between jihadist militant networks and the Malian state. Grievances regarding economic and political exclusion are found in areas where perceptions of marginalization are very strong among local populations, "providing both a motivation and an opportunity for collective opposition."[117] In areas like Kidal, militants can make use of previous experience with violence as a means for political expression and easily recruit members to act violently for a new project in a new strategic framework.[118] Dowd's data from regions with high rates of violence in Kenya, Mali and Nigeria show that Islamist violence often occurs in areas where people feel marginalized and not able to benefit from national politics and economic opportunity. In these regions, historic developments have proved for local actors that violence can create positive results. "The very language and targeting of Islamist violence cannot be divorced from domestic politics and historical violence in the state."[119] Not only can we find strong jihadist militant networks in northern Mali, we also find strong criminal networks operating in all corners of Mali and the Sahel. Tinti writes:

> The international community will need to recognize the extent to which illicit trafficking and organized crime influences broader security and governance issues. And with this change should come the recognition that many of the people the international community consider partners in the quest to rebuild Mali—politicians, traditional leaders, the military—are themselves implicated or complicit in illicit trafficking and organized crime.[120]

Perspectives for the peace process in Mali

If Kilcullen and Guichaoua are right in their descriptions of the dynamics of the Tuareg insurgency, the peace process in Mali will proceed more smoothly with their analytical points incorporated.[121] Today, the peace process negotiations isolate some groups outside the process as terrorists. In reality, these jihadist militant groups are networks and individuals working through existing social and family structures in Kidal, Gao and Timbuktu. Replacing the label terrorist with the label "bricoleur" seems valid in the sense that these ad hoc militant groups operate through the clan structure, local politics and trade networks. The jihadist militant groups are funded by kidnappings and smuggling, and are seen as both investors and security providers by the local population, who are dependent on income from the criminal economy. Therefore, MINUSMA and the Malian government should consider militant groups as important actors. Given the pragmatic flexibility of their members, long-term negotiations for peace must include the major parts of the supporters and members of the jihadist militant groups in the region. The ad hoc nature of militant groups in northern Mali also represents a possible aid for MINUSMA's stabilization efforts. Loose loyalties make it easy for fighters to leave an armed group if they can see better options in a neighboring group or alternative opportunities. This phenomenon points to a tactic allowing MINUSMA to actually benefit from the "hop-on—hop–off" mobilization of fighters when trying to de-mobilize and disarm fighters, and create a stable environment for the people of Mali.

Notes

1. European Commission Humanitarian Aid Decision (ECHO), 11th European Development Fund (EDF), Decision reference no. ECHO/-WF/EDF/2015/02000, "Commission decision financing humanitarian actions in Mali and neighboring countries Burkina Faso and Mauretania from the 11th EDF," 2015.

2. United Nations, MINUSMA Mission Homepage: Facts and Figures, 2013, http://www.un.org/en/peacekeeping/missions/minusma/facts.

3. Morten Bøås, "Castles in the sand: Informal networks and power brokers in the northern Mali periphery" in *African Conflicts and Informal Power: Big Men and Networks*, ed. Mats Utas (New York: Zed Books, 2012); Grégory Chauzal and Thibault van Damme, *The Roots of Mali's Conflict. Moving Beyond the 2012 Crisis*, CRU Report (Oslo: Clingendael, 2015); Caitriona Dowd, "Grievances, governance and Islamist violence in sub-Saharan Africa," *Journal of Modern African Studies* 53, no. 4 (2015): 505–531, DOI: https://doi.org/10.1017/S0022278X15000737 ; Wolfram Lacher, *Organized Crime and Conflict in the Sahel-Sahara Region*, Carnegie Endowment for International Peace paper, 13 September 2012, http://carnegieendowment.org/2012/09/13/organized-crime-and-conflict-in-sahel-sahara-region-pub-49360; Francesco Strazzari, *Azawad and the rights of passage: the role of illicit trade in the logic of armed group formation in northern Mali*, NOREF Report (Oslo: Clingendael, 2015); Peter Tinti, *Illicit Trafficking and Instability in Mali: Past, Present and Future*, Global Initiative research paper (Geneva: The Global Initiative Against Transnational Organized Crime, January 2014), 1–19.

4. This author uses the term 'jihadist militant groups' instead of the term 'terrorist armed groups' used by the Malian government and most MINUSMA staff. The discussion of the concept 'terrorist' will appear later in the article. In addition, he does not list the different militant groups in Mali because there is a risk that half a year from now, new groups will have emerged and others disappeared. What is important here is the social and economic dynamics triggering the violence.

5. This article has benefitted greatly from comments and critique by Professor Thomas Mandrup and Assistant Professor Thomas V. Brønd at the Royal Danish Defence College, civil analyst Susanne Vedsted, Danish Army and consultant Nina Nellemann Rasmussen from the University of Copenhagen. Several Danish officers supported my fieldwork in Bamako and Gao. Thanks to all of them for their hospitality and interest in this study. A special thanks to Rasmus and Andreas, our talks were very inspirational.

6. Michael T. Flynn, Matthew F. Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington: Center for New American Security, January 2010).

7. Mya Mynster Christensen, Rikke Haugegaard, and Poul Martin Linnet, *War amongst the People and the Absent Enemy: Towards a Cultural Paradigm Shift?*, research paper, (Copenhagen, RDDC, October 2014), http://www.fak.dk/publikationer/Documents/War-amongst-the-people.pdf.

8. Mats Utas, "Introduction. Bigmanity and network governance in African conflicts," in *African Conflicts and Informal Power: Big Men and Networks*, ed. Mats Utas (New York: Zed Books, 2012), 1–34.

9. Carolyn Nordstrom, "Shadows and Sovereigns," *Theory, Culture and Society* 17, no. 4 (2000): 35–54.

10. Mats Utas, "Introduction."

11. At the time of my fieldwork, the ASIFU headquarters in Bamako consisted of a 70 person unit covering analysis and fusion, command and control, and logistics capacity. There was also an open sources section monitoring newspapers, TV, web-based news and social media. The ASIFU contained two intelligence, surveillance and reconnaissance (ISR) units in Gao (covering Gao (Sector East) and Kidal (Sector North) and Timbuktu with sensor and analysis capacity, human intelligence and drones: John Karlsrud and Adam C. Smith, "Europe's Return to Peacekeeping in Africa? Lessons from Mali," in *Providing for Peacekeeping* (New York: International Peace Institute, 2015), 11. In 2016, the UN HQ in New York decided to merge the two major units in MINUSMA working with intelligence analysis—the ASIFU and the U2—into one single unit. The merge took place in order to combine efforts of long-term analysis (the ASIFU) with daily, current analysis (U2 in MINUSMA HQ)—high ranking officer in MINUSMA HQ, interview with author, June 2016.

12. Arthur Boutellis, "Can the UN Stabilize Mali? Towards a UN Stabilization Doctrine?," *Stability: International Journal of Security & Development* 4, no. 1 (2015): 11, DOI: https://doi.org/10.5334/sta.fz 33.

13. World Food Programme, WFP Mali Brief, 2015, http://www1.wfp.org/countries/mali.

14. European Commission Humanitarian Aid Decision (ECHO), 2.

15. United Nations, "Accord Pour La Paix et la Reconciliation au Mali," 1 March 2015. Document copy from field study in MINUSMA.

16. Marko Scholze, "Between the Worlds: Tuaregs as Entrepreneurs in Tourism: Tuareg Moving Global," in *Tuareg Society within a Globalized World: Saharan Life in Transition*, eds. Anja Fischer and Ines Kohl, Book 91 (London: I.B. Tauris, 2010), 174.

17. Yvan Guichaoua, "Circumstantial Alliances and Loose Loyalties in Rebellion Making: The Case of Tuareg Insurgency in Northern Niger (2007–2009)," in *Understanding Collective Political Violence,* ed. Yvan Guichaoua (London: Palgrave Macmillan).

18. Wolfram Lacher, *Organized Crime and Conflict in the Sahel-Sahara Region*, 9; Modibo Goïta, "West Africa's Growing Terrorist Threat: Confronting AQIM's Sahelian Strategy," *Africa Center for Strategic Studies*, Africa Security Brief no. 11 (February 2011): 2

19. European Commission Humanitarian Aid Decision (ECHO), 2.

20. UN General Assembly Security Council, "Children and armed conflict, report of the Secretary-General," 5 June 2015, S/2015/409, para 22, https://reliefweb.int/sites/reliefweb.int/files/resources/N1510923.pdf.

21. Modibo Goïta, "West Africa's Growing Terrorist Threat," 3.

22. Manni Crone, *Militante islamistiske grupper i Mali. Ideologi, strategi og alliance* (Copenhagen: Danish Institute for International Studies 2013), 13.

23. Olivier Guitta, "Al-Qaeda in the Islamic Maghreb: A Threat for the West," *Defence Against Terrorism Review* 3, no. 1 (2010): 56.

24. Ibid.

25. UN Security Council Report, "Africa, Mali," 23 December 2014), www.securitycouncilreport.org.

26. Arthur Boutellis, "Can the UN Stabilize Mali?," 6.

27. Modibo Goïta, "West Africa's Growing Terrorist Threat," 4.

28. Ibid., 5.

29. Olivier Guitta, "Al-Qaeda in the Islamic Maghreb," 64.

30. Ibid., 56.

31. Danish officer previously working in MINUSMA, briefing with author, May 2015.

32. Bøås, "Castles in the sand," 124.

33. Tinti, *Illicit Trafficking and Instability in Mali*, 15.
34. Manni Crone, *Militante islamistiske grupper*, 13.
35. Hannah Armstrong, "Winning the War, Losing the Peace In Mali: After the Fighting, Mali's Ethnic Tensions Continue to Fester," *New Republic*, 28 February 2013, https://newrepublic.com/article/112539/malis-ethnic-tensions-fester-after-fighting.
36. MINUSMA officer, interview with author November 2014.
37. Olivier J Walther and Dimitrios C. Christopoulos, "Islamic Terrorism and the Malian Rebellion," Terrorism and Political Violence 27, no. 3 (2014): 497–519, DOI: https://doi.org/10.1080/09546553.2013.809340.
38. Ibid., 503, cited in Renée C. van der Hulst, "Terrorist Networks: The Threat of Connectivity," in *The SAGE Handbook of Social Network Analysis*, eds. John Scott and Peter J. Carrington (London: Sage, 2011).
39. Ibid., 503.
40. MINUSMA staff, interview with author, October 2015.
41. Danish linguist, e-mail interview by author, August 2016.
42. Bøås, "Castles in the sand," 128–129.
43. Mats Utas, ed., *African Conflicts and Informal Power: Big Men and Networks* (New York: Zed Books, 2012), 1–34.
44. Marshall Sahlins, "Poor Man, Rich Man, Big-Man, Chief: Political Types in Melanesia and Polynesia," *Comparative Studies in Society and History* 5 (1963): 289.
45. Ibid.
46. Utas, "Introduction," 6, citing Maurice Godelier, *The Making of Great Men: Male Domination and Power Among the New Guinea Baruya* (Cambridge: Cambridge University Press, 1986), 163.
47. Utas, "Introduction," 6, citing AbdouMaliq Simone, "People as Infrastructure: Intersecting Fragments in Johanesburg," *Public Culture* 16 (2004): 407.
48. AbdouMaliq Simone, *For the City Yet to Come: Changing African Life in Four Cities* (Durham, NC: Duke University Press, 2004), 81.
49. MINUSMA staff, interview with author, 2014.
50. Utas, "Introduction," 8.
51. Bøås, "Castles in the sand," 125.
52. Henrik E. Vigh, "Navigating Terrains of War. Youth and Soldiering in Guinea-Bissau," in *Methodology and History in Anthropology* (New York: Berghahn Books, 2007), 13.
53. Ghassan Hage in Ibid., 104.
54. Tuesday Reitano and Mark Shaw, *People's perspectives of organized crime in West Africa and the Sahel*, paper 254, (Pretoria, South Africa: Institute for Security Studies, April 2014), 6.
55. Guichaoua, "Circumstantial Alliances and Loose Loyalties in Rebellion Making," 15, 21.
56. Crone, *Militante islamistiske grupper*. Translation by author.
57. Boutellis, "Can the UN Stabilize Mali?," 6–7.
58. Ibid., 10.
59. Utas, "Introduction."
60. Guichaoua, "Circumstantial Alliances and Loose Loyalties in Rebellion Making," 6.
61. David Kilcullen, "Counterinsurgency Redux," *Survival* 48, no. 4 (2006): 7.
62. Ibid.
63. Chauzal and van Damme, *The Roots of Mali's Conflict*, 50.
64. Kilcullen, "Counterinsurgency Redux," 6.
65. Bøås, "Castles in the sand"; Crone, *Militante islamistiske grupper*; Guichaoua, "Circumstantial Alliances and Loose Loyalties in Rebellion Making."
66. Utas, "Introduction."
67. Crone, *Militante islamistiske grupper*.
68. Utas, "Introduction," 6, citing AbdouMaliq Simone.
69. Groupe Salafiste pour la Prédication et le Combat. GSPC, originally from Algeria, merged with Al-Qaeda in 2007 to form the group Al-Qaeda in the Islamic Maghreb (AQIM).
70. Guitta, "Al-Qaeda in the Islamic Maghreb," 66.
71. Goïta, "West Africa's Growing Terrorist Threat," 3, citing Stephanie Plasse, "Tuareg and AQIM: The Unlikely Jihadist Bedmates," *Afrik News*, 8 November 2010.
72. Ibid.
73. Guitta, "Al-Qaeda in the Islamic Maghreb," 59.

74. Ben Anderson, "Facing the Future Enemy: US Counterinsurgency Doctrine and the Pre-insurgent," *Theory, Culture & Society* 28, no. 7–8 (2011): 221, DOI: https://doi.org/10.1177/0263276411423039.
75. Ibid.
76. Goïta, "West Africa's Growing Terrorist Threat," 3.
77. Lawrence E. Cline, "Nomads, Islamists, and Soldiers: The Struggles for Northern Mali," *Studies in Conflict & Terrorism* 36, no. 8 (1 August 2013): 617-34, https://doi.org/10.1080/1057610X.2013.802972.
78. Dowd, "Grievances, governance and Islamist violence in sub-Saharan Africa," 519–520.
79. Goïta, "West Africa's Growing Terrorist Threat," 5.
80. Chauzal and van Damme, *The Roots of Mali's Conflict*.
81. Walther and Christopoulos, "Islamic Terrorism and the Malian Rebellion," 506–508.
82. Crone, *Militante islamistiske grupper*, 10.
83. Julius Cavendish, "The Fearsome Tuareg Uprising in Mali: Less Monolithic than Meets the Eye," *TIME*, 30 March 2012.
84. Bøås, "Castles in the sand."
85. MINUSMA officer, personal communication with author, 2014.
86. UN Security Council Report, "Assessment Mission on the Impact of the Libyan Crisis on the Sahel region," 2012, 11.
87. Kwesi Aning and John Pokoo, *Drug Trafficking and Threats to National and Regional Security in West Africa*, WACD background paper 1, (Accra: West Africa Commission on Drugs, 2013), 8, http://works.be press.com/kwesi_aning/2/.
88. Lacher, *Organized Crime and Conflict in the Sahel-Sahara Region*, 913; Goïta, "West Africa's Growing Terrorist Threat," 4.
89. David Lewis and Adama Diarra, "Special Report: In the land of 'gangster-jihadists,'" *Reuters*, 25 October 2012, https://www.reuters.com/article/us-mali-crisis-crime/special-report-in-the-land-of-gangster-jihadists-idUSBRE89O07Y20121025.
90. Lacher, *Organized Crime and Conflict in the Sahel-Sahara Region*; Aning and Pokoo, *Drug Trafficking and Threats to National and Regional Security in West Africa.*
91. Nordstrom, "Shadows and Sovereigns."
92. Ibid., 42.
93. Lacher, *Organized Crime and Conflict in the Sahel-Sahara Region*, 12–15.
94. Nordstrom, "Shadows and Sovereigns,"40.
95. Aning and Pokoo, *Drug Trafficking and Threats to National and Regional Security in West Africa*, 5.
96. Goïta, "West Africa's Growing Terrorist Threat," 2.
97. UN Office on Drugs and Crime, "Transnational Organized Crime in West Africa: A Threat Assessment," 2013, 11.
98. Aning and Pokoo, *Drug Trafficking and Threats to National and Regional Security in West Africa*, 5.
99. MINUSMA meeting, Gao, 2014.
100. Strazzari, *Azawad and the rights of passage*, 3-4.
101. Ibid.
102. Boutellis, "Can the UN Stabilize Mali?," 7.
103. Ibid.
104. Ibid.
105. Strazzari, *Azawad and the rights of passage*, 7.
106. Lacher, *Organized Crime and Conflict in the Sahel-Sahara Region*, 5.
107. Crone, *Militante islamistiske grupper*; Strazzari, *Azawad and the rights of passage*.
108. Bøås, "Castles in the sand," 131.
109. Strazzari, *Azawad and the rights of passage*, 4, citing Pietro Musilli and Patrick Smith, *The lawless roads: an overview of turbulence across the Sahel*, NOREF Report (Oslo: Clingendael, 2013).
110. Ibid.
111. Dowd, "Grievances, governance and Islamist violence in sub-Saharan Africa," 506.
112. Boutellis, "Can the UN Stabilize Mali?," 5.
113. Ibid., 6.
114. Ibid.
115. Ibid.
116. Danish Ministry of Foreign Affairs, "Seminar on Mali," Copenhagen, Denmark, 31 March 2016.
117. Dowd, "Grievances, governance and Islamist violence in sub-Saharan Africa," 519.
118. Ibid., 520.
119. Ibid., 521.

120. Tinti, *Illicit Trafficking and Instability in Mali*, 19.

121. Kilcullen, "Counterinsurgency Redux,"; and Guichaoua, "Circumstantial Alliances and Loose Loyalties in Rebellion Making."

Foundations of Economic Theory

Money, Markets and Social Power

Garry Jacobs*

Less than a decade after the most severe global economic crisis in a century, the world economy is once again veering toward the edge. Economists, central bankers, corporate leaders and politicians are scrambling to understand and respond to the threat. But as in 2008, debate focuses on how to tinker and patch up holes in the existing system. Few are willing to recognize the deeper implications. Centrally planned economies were discredited a quarter century ago, leading to a resurgence of neoliberal theory and public policy that dismantled social welfare systems, disempowered labor unions, liberated the wealthy from the burden of taxation, and enabled multinational corporations to stalk the earth unhindered by competition and rule of law. Prevailing economic philosophy is a reversion to obsolete concepts and policies.

The call for New Economic Theory arises from many sources and resonates with many different concerns. The present crisis has exposed the inherent fault-lines and structural deficiencies of the existing economic model. Meanwhile most economists remain preoccupied with theorizing about what went wrong within the confines of the existing theoretical framework rather than re-examining the fundamental premises on which it exists and looking beyond for a more viable alternative. Ten years ago such a call would have met with derision from leaders, economists and the public-at-large. Today there is a growing sense of unease, inklings of Hamlet's deeper perception that all is not well within the state of Denmark. A shift in focus is needed from efforts to reinforce an inherently flawed and failing system to conceptualizing a better one. That necessitates a reexamination of the social and political foundations of modern economic systems to fathom the underlying forces that have shaped their development and are now driving evolution to something else.

The quest for new theory needs to lay bare both the explicit assumptions and implicit premises on which current theory resides. It needs to reject the notion of immutable economic laws in favor of the concept that economic systems are human

*Chief Executive Officer, World Academy of Art & Science; Vice-President, The Mother's Service Society, Pondicherry, India; International Fellow, Club of Rome.

Garry Jacobs, "Money, Markets and Social Power," *Cadmus* 6, no. 2 (May 2016): 20-42. Available at: http://cadmusjournal.org

constructions framed under the pressure of prevailing circumstances and forces in the past and, therefore, capable of continuous evolution and radical improvement. Formulation of new theory should commence with a thorough re-examination of economy from first principles. In an age of rapid globalization, accelerated social evolution and unprecedented integration, it is necessary to re-examine the narrow spatial, temporal and conceptual boundaries that circumscribe current economic concepts, models, institutions and policies. The future science of Economics must necessarily be global rather than national in scope and evolutionary rather than static in perspective. It needs to be fundamentally interdisciplinary in order to fully embrace the increasingly complex sectoral interconnections that characterize modern society. It must also delve beneath the surface of economic activities and institutions to identify the transdisciplinary principles of social existence and development which constitute the theoretical foundation for all the human sciences.

This paper examines three fundamental aspects of modern economy to illustrate the types of issues and perspectives relevant to a reformulation of Economics. It seeks to frame the functioning of economy within a broader political, social, cultural, psychological and ecological context. It seeks to unveil underlying social forces responsible for the present functioning of economies, which can be effectively addressed and controlled only when they are made conscious and explicit. The notion that economies work the way they do because of intractable social forces may be deemed expedient by practitioners, but it cannot serve as the basis for valid scientific theory. Economy and Economics are both human inventions. Whatever the forces that have shaped their development in the past, the only legitimate objective of economic science is a system of knowledge that promotes the welfare and well-being of all humanity.

The central argument of this paper is that markets and money are remarkable inventions designed to organize human relationships into power for social accomplishment. They are instruments for the conversion of social potential into social power. They harness the power of organization to transform human energies into social capacity. The distribution of rights and privileges in society determines how these social institutions function and who benefits. Freedom means access to social power and is only possible in the measure all forms of that power—political, economic, and social—are equitably distributed. The current system is inherently biased in favor of privileged elites reinforcing domination by the more powerful. Fullest development of individual and social welfare can only be achieved in conditions of freedom and equality. Economic theory needs to make explicit the underlying forces determining the distribution of power and its benefits, so that conscious policy choices can be made to reorient markets and money to serve their intended purpose promoting human welfare and well-being.

We start with the premise that the purpose of any economic system is to maximize the economic security, welfare and well-being of its citizens. In comparison with

the past, the current system has had remarkable success providing unprecedented levels of prosperity to an expanding global population. Any critique of the current system must commence with a deep appreciation of its achievements.

The Market

Modern market economies are a subset and component of a much larger set of social institutions on which economy is founded and depends for its accomplishments. The birth of the primordial market was a simple device designed to bring buyers and sellers together at a specific place and time to exchange goods. The traditional village fair gradually coalesced into centralized urban market centers linking different regions of the countryside with one another and through sea and land routes to more distant places. The rise of the annual cycle of Champagne Fairs during the Middle Ages marked an early stage in the emergence of All-European markets based on the same principle.

The wealth of modern economies is founded on the ever-expanding organization of human relationships. The market is a simple but extremely powerful example of social organization that acts as a catalyst for production by stimulating exchange. Before markets, farmers had little incentive to produce anything more than they required for personal consumption and local exchange. Markets broaden and elevate the power of economies by shifting the center from production to exchange.

The creation of markets transformed subsistence agriculture into commercial agriculture by providing farmers with an incentive to maximize production and exchange it for an increasing diversity of essential and exotic goods. Eugen Weber documents how grape farmers in an isolated corner of rural France without access to regional markets used to feed their excess grape production to the pigs, since there was only so much fruit and wine they could consume locally. Within a year after bridges and roads were constructed connecting the village with wider markets, they were exporting wine to the Middle East.[1] Adam Smith recounts the time before improvements in transportation supported the development of national markets in Scotland. Feudal barons controlling large extents of land had little incentive to increase production beyond the level needed to feed their families and large contingents of armed retainers, since surplus production beyond this level had little value. Once connected to urban markets, large landholders drastically reduced the number of their dependents—in one case from several thousand to just 50—in order to convert surpluses into a wide range of luxury goods.[2]

All social accomplishment is the result of the process of generating, releasing, directing and channeling human energies by organizing and coordinating the interactions and relationships between individuals, activities, and institutions. The immense capacity of market economies for production and innovation arises out of the freedom of choice and action they accord for individual initiative and innovation and for organized and

finely coordinated collective action. Freedom liberates productive human energies. Market opportunities direct those energies for productive purposes. The evolution of intricate networks of markets at the local, regional, national and international levels channels those energies effectively to maximize the production and exchange of goods and services. The spatial expansion of markets enhances the range and variety of goods available and enables buyers to source products from producers with the greatest comparative advantage.

From earliest times, economy and politics have been inextricably intertwined. Freedom of production and exchange meant little without ensuring ownership and security of property, enforcing contracts, arbitrating disputes, and protection against arbitrary seizure. The most productive market economies developed in places where the rights of the individual, rule of law and protection for property were most respected. Thus, democracies and market economies evolved hand-in-hand and were mutually reinforcing. So too, markets thrived in communities with the best infrastructure for transportation and communication, as well as the most skilled, literate and well-educated people.

At a time when the power of monarchs and emperors far exceeded the capacities of any commercial enterprise, Smith opposed the mercantile policies of European governments which promoted the interests of the crown and a small community of prominent traders at the expense of the general public. He never imagined the emergence of huge multinational corporations whose economic and political power would exceed the wealth and influence of many nations and even have the capacity to undermine the ecosystem of the planet. The rise of huge trading corporations during the 18th century and private transcontinental railways and massive industrial enterprises during the 19th century shifted the balance of power and the source of threat to free markets from governments to producers, traders and transporters. The multiplication of social power generated by the Industrial Revolution generated unprecedented economic capacity while posing new threats to human freedom and creativity.

The development of market economies during the 20th century is inseparable from the development of political systems to govern the actions of enterprises, educational systems to provide the skilled manpower required, scientific research institutions to support rapid technological innovation in products and production, continuous advances in transportation and communication, combined with a dense fabric of laws and judicial mechanisms to define and protect rights and responsibilities, preserve competition, ensure fair treatment of workers and consumers, protect and support communities, and safeguard the environmental rights of present and future generations.

The enormous productive power of modern economies is a subset and an inseparable element of the growing power of an increasingly sophisticated and complex global social organization encompassing virtually all aspects of human existence. Modern economies

have evolved in conjunction with stable national governments, democratic systems of governance, peaceful international relationships supported by rapid development of international law and an expanding network of international institutions, transparent judiciary systems, banking and market regulatory institutions, independent media, systems of education and research, social welfare systems, consumer and environmental protection agencies, and a plethora of other organizations.

The central importance of this underlying social fabric is dramatically illustrated by recent attempts to rapidly introduce market economies in countries that lack the capacity for democratic governance, rule of law, and social justice. The history of Ukraine and other countries of the former Soviet Union over the past 25 years present startling evidence of how totally dependent development of an equitable market economy is on the prior and proportionate development of all the other institutions of modern social organization.[3]

Myths of the Market

However remarkable and unprecedented its achievements, by comparison with any conception of optimality, the present market economic system fail to impress. Judged in terms of its contribution to maximizing the security, welfare and well-being of all citizens, it dismally fails to effectively harness the superabundance of available productive capacity to meet the ever expanding needs and aspirations of the world's population. It fails to effectively develop and fully engage the precious and perishable human capital which represents the foundation, peak and core of humanity's advancing civilization and culture. Today approximately 200 million workers are unemployed and an estimated billion or more are underemployed. The labor force participation rate is falling while youth unemployment is rising. The present system fails to ensure an equitable distribution of the extraordinary benefits of modern economic processes to all human beings. Levels of economic inequality have risen to their highest in nearly a century. Meanwhile the basic needs and aspirations of billions of people remain unmet and levels of poverty are rising in some regions. The system fails to provide the level playing field which is the *sine qua non* for a true market economy. Multinational corporations enjoy unprecedented freedom from national accountability in a wild west of globalization. Mergers and acquisitions are restricting competition on a global scale. The present system also fails to effectively utilize financial capital for the welfare of society. Today, the supply of money is superabundant but only a small portion of it is utilized for productive investment. Out of approximately $250 trillion in global financial assets, probably less than 20 percent is actively engaged to support the real economy.

However impressive today's achievements by historical standards may be, they fail to impress when compared with the magnitude of unmet needs and underutilized capacities. All these failings are symptoms of an economic system increasingly di-

vorced from human needs and the welfare of society. Financial markets which are intended to serve and support development of the real economy have become autonomous and increasingly divorced from it. The unbridled application of new technologies has created a rapidly widening gap between production and employment at a time when welfare systems have been cut back and individuals possess no alternative means of meeting their consumption needs. Economic activity is increasingly threatening the security of individuals, the stability of society and the sustainability of the planetary environment.

Perhaps the most compelling argument given in support of the existing market economic system is that it is better than the known alternatives. There was a time when it could well be said that monarchy was better than the alternative of a politically divided system of independent feudal barons or when the introduction of coinage represented a considerable advance over barter. That has been true of thousands of social advances in the past, each of which in turn has been eventually superseded by something better.

The deep appeal of the market economic system stems from its association with universal human values. The market is a compelling symbol of freedom, self-reliance, individuality, innovation, and creativity. By eliminating the intervention of self-enriching, tyrannical monarchs, it presents itself as the democratization of economy. Basing itself on universal principles, it purports to be guided by the social equivalent of the universal laws of nature discovered by science that govern the natural world.

The intellectual appeal of neo-classical economic theory is a mirage founded on prevailing myth and profound misconceptions which prevent intelligent debate. The market economy is not a phenomenon of nature but a creation of humanity. It is not founded on immutable universal laws, but rather on principles and rules formulated by human beings to serve specific interests, which continuously shift over time. The market economy is not a construction of God or Nature. It is a social construction of reality and our understanding of it is powerfully influenced by socially constructed ways of thinking. In quest of a natural science of economy, the Newtonian equivalent of the laws of motion, Economics is based on the conception of a mechanized, clockwork system miraculously independent of the consciousness of the human beings by whom it has been fashioned, who formulate the rules by which it is governed, and who make the countless decisions by which it functions. We attribute almost mystical powers to the market to rationally maximize efficiency and human welfare with impartial equity and justice for all. But these powers are largely mythical. The notion of markets as impartial, unbiased, independent playing fields is a fabricated illusion.

Markets as they function today are not rational, fair, equitable or efficient, and they certainly do not maximize human welfare. The notion of fairness and equity is undermined by patent and copyright laws, which according to *The Economist,* accord rights far beyond what has been proven to be socially beneficial.[4] It is distorted by

uncompetitive monopolistic practices, excessive consolidation of industries by M&As, and tax policies that favor capital investments or employment of people and the wealthy over other income groups. It is subject to powerful influence by the lobbying of vested interests, the temptations and allurement of corrupt politicians, and biased procurement practices. It is biased by the rent-seeking of a plethora of privileged communities, including licensed professionals, which permeates the entire policy environment governing the operations of the market. For instance, an artificial constraint on the number of medical school seats in the U.S., which has remained flat from 1980 to 2006 despite a 37 percent increase in the population, allows doctors to extort higher prices from middle class Americans.[5] *The Washington Post* recently drew attention to the obscure example of dentists in the USA who have exercised their influence to maintain monopolistic prices more than twice the market level on non-medical practices such as tooth whitening.[6]

The efficiency of markets is largely a question of one's definition and bookkeeping. Markets do indeed encourage efficient means of production when narrowly defined at the level of the firm. At the same time they foster socially wasteful competitive activity and generate huge social costs, which are treated as externalities. The bias for capital and energy-intensive technologies over labor is not a law of nature, but rather a consequence of policies that incentivize capital investment, tax labor, price energy far below its true replacement cost, and ignore the true social costs of pollution. While the firm may maximize efficiency by replacing labor with machinery, society as a whole incurs enormous financial and social costs resulting from rising levels of unemployment and underemployment, poverty, crime, physical and mental illness, social alienation and violence. A study by Randall Wray in the USA estimated that the social costs of rising levels of unemployment equal or exceed the direct cost of employing people.[7]

As economist and former investment banker Tomas Björkman points out in his book *Market Myths*, our adherence to orthodoxy prevents us from seeing the glaring gaps between the myth of the market and the highly unrealistic assumptions on which the neo-classical economic model is constructed, on these theoretical models and the actual way in which markets work, and on the way markets work now and alternatives that could be created while remaining within the framework of market economies.[8] Economists are so preoccupied with understanding the minuscule characteristics and idiosyncrasies of the present system that little thought is directed toward questioning the basic premises on which it is based or on exploring more attractive alternatives.

Economics is still governed by a mythical concept of market equilibrium. If markets tend toward equilibrium, why is economic inequality rising to historically high levels? Why have multinational corporations consolidated domination of one global market after the other? Why has oil soared to $150 a barrel and then fallen to

$30 a barrel within a short period of time? Why do financial and property markets swing so widely from one extreme to another? Why do central banks have to suppress irrational exuberance and then try to stimulate higher investment and consumption? Why is unemployment rising inexorably in spite of the dismantling of protective labor legislation in many countries? The Newtonian conception of a world in equilibrium was rejected by physicists a century ago. Today it is universally accepted that we live in an evolving and rapidly expanding universe. The conception of eternally static forms of life was replaced by Darwin's conception of biological evolution in the 19th century. The startling speed of scientific and technological evolution is too blatantly apparent to require illustration. Yet economic theory clings to a concept of static equilibrium by externalizing the powerful forces compelling the rapid evolution of the entire global political, economic and social system.

It is understandable that the wealthy, the corporate sector, politicians dependent on them and central bankers obeying narrow constitutional mandates should cling to the present dogma and endeavor to hold it above scrutiny or reproach. But that does not explain why the vast majority of economists engage themselves in analysis and tinkering rather than in-depth questioning of the underlying premises and efforts to conceptualize a better alternative.

Evolution of Human-centered Economics

Society evolves by a progressive organization of human activities to an increasing extent in space and time, with increasing coordination between its myriad activities and increasing integration between the multiple layers of the social fabric. The market is an extraordinary product of human ingenuity, a social organization capable of managing inconceivable and ever increasing levels of interconnectedness and complexity with ever greater velocity and precision. Yet it is only a form of social technology. Like democracy and other forms of social technology, *its value depends on the central purpose for which it is applied, the values by which it is guided and the principles on which it is founded.*

The failings of mainstream economic theory recounted above are really minor in comparison with its most fundamental flaw—deviation from its central purpose. Social institutions are created to serve society. That is their rightful claim to legitimacy. Yet they have a nearly irresistible tendency to diverge from that intended purpose over time, as the church, the state, the military and other institutions have so often done. Like other institutions, the market has veered from the intended purpose which Smith extolled and has been diverted to serve powerful vested interests. That purpose can and must be restored. It may be argued by some that markets have always functioned in this manner subject to the same distortion, just as governments have always served the interests of an élite, regardless of their proclaimed ideals. This is indeed the case, but does not weaken the justification for rectification. Just because every democ-

racy has failed in its pursuit of liberty, equality and justice for all, that does not justify the *status quo*. Rather it calls for evolutionary or revolutionary action to realize the original ideal.

What is needed now is nothing less than a Copernican Revolution in Economics to liberate our minds from the myths, illusions and misconceptions on which current theory is founded. But this should be a revolution in reverse. Copernicus challenged the anthropocentric, geocentric conception of the physical universe that grossly distorted and exaggerated the place of earth and humanity in the universal scheme of things. Instead, he projected a heliocentric perspective that placed earth as a mere satellite of the sun, a tiny dot in an infinite universe. Humanity was dethroned from its place at the center. It was a humbling experience for God's chosen. In contrast, the prevailing economic model perversely positions the market, money and technology at the center and places the interests of humanity at the periphery. Its goal is to maximize economic activity, not human security, welfare or well-being. It thrives on unlimited consumption and mindless ecological destruction. It maximizes accumulation of wealth among a few, rather than dissemination of economic welfare among all. It worships illusory Gods of the market and attributes unassailable wisdom to blatantly flawed processes. *Reversing the model, we need to reposition human beings at the center of economic theory and conceive of a market system that will maximize the freedom, security, and welfare of all people.*

The choice is not simply between regulated and self-organizing free markets. Self-organizing markets are rarely or never free. The self-organizing character of the Internet does not prevent a few giant firms from controlling an increasing share of all web traffic and revenues. Free markets exist and only exist within the structure provided by democracy, rule of law and regulatory authority. Regulations that enforce rules of law, fair practices, humane standards and prevent monopoly are essential to the operation of a market economy. But that does not mean that direct regulatory intervention by government is required for the smooth functioning of every market. Much can be done by ensuring the laws and rules governing the operation of markets are fair and equitable.

A historical perspective on the origin and development of current laws and practices will make evident that other social forces have continuously intervened to distort the workings of the market in favor of the privileged and powerful. That is why a true science of economy has to be founded on a science of society which comprehends the sources of social power and the means by which the rightful exercise of that power is diverted to serve the interests of a privileged class.

The debate between public and private good is misconceived. *Markets are founded on fundamental principles of human relationship and social organization.* All knowledge, all wealth, all discovery and invention are the product of collaboration between enterprising individuals and the communities in which they function. *There can be no opti-*

mal private good for all individuals in this world without simultaneously optimizing the benefit to society as a whole. Every individual achievement is founded on the cumulative achievements of all humanity over millennia. Digital computing today owes its astounding accomplishments to invention of the zero, Hindu numerals and decimal place by Indian mathematicians more than 1600 years ago and their transmission by Persian scholars some four centuries later. Nothing can be thought, expressed, invented or produced without drawing on that universal reservoir of social wealth. So too, there can be no social advancement, discovery, innovation or creativity without the aspiration, inspiration and invention of creative individuals.

Markets have evolved from rudimentary origins in the distant past. In addition to growing in scale, diversity and complexity, they have also become more equitable and humane over time. There is no reason to think that the present system is the most just and perfectly attainable. Rather there is every reason to believe it is a partial and highly imperfect form of a social system with immense potential for further evolutionary advancement. The increasing concentration of wealth today and divergence of money from the real economy impose severe constraints on the further development of economic prosperity worldwide. Democracy has proven a far more powerful and stable form of government than any monarchy because it enables every citizen to enjoy political rights and freedoms. So too, market economies can only fully realize their potential for wealth generation when they create opportunities for all citizens to productively contribute and enjoy the benefits of society's labors.

Social systems evolve along multiple dimensions. The quantitative capacity, geographic reach and speed of operation of every system are a function of organization and technology. The qualitative values they manifest are a function of conscious awareness, choice and political will. A human-centered science of Economy needs to reexamine the purpose, values and principles on which the market economy functions to optimize its capacity to meet human needs, promote human welfare and foster human evolution.

Money

What is true of markets is equally true of money. Conventional economic theory describes the function of money as a means of exchange, unit of account and store of value. But this oft repeated formula fails to describe the reality of money or to adequately explain its remarkable powers as a catalyst for economic, social and human development. A fuller understanding of the reality of money reveals the enormous scope for more effectively harnessing its creative powers to promote economic and social welfare. Its most fundamental contribution is to human psychological development, which is the ultimate aim of civilization.

Money as Organization

The power of money arises from the fact that it is a social organization in the same way language, market, and the Internet are social organizations. Language is an organized system of letters, words and sounds. The words we use have no intrinsic value other than the value we assign to them by social convention and psychological association. The power of words arises from the fact that they carry a commonly shared meaning. If each person had his or her own language, it would be useless for communication with others. The more widely a language is shared, the more powerful its words as a medium of communication. Social convention rather than intrinsic value makes words powerful.

The same is true of money. Most people regard money as a thing, even though most of the money we utilize today no longer takes the form of a tangible object. Money is not a thing in itself. It is a social convention for harnessing and organizing the power of human relationships which derives its power from the fact that the convention is shared. The development and acceptance of a common convention and standard of acceptability of money have evolved over many centuries. That convention is made possible by the institutions that issue it in standardized forms; the laws that govern its issuance, acceptance as legal tender and the rights of ownership; the procedures and mechanisms for its transference, transport, storage and convertibility; methods of accounting for it, lending and borrowing, etc.

The power of money arises not from any intrinsic value of its own, but from the complex social organization which supports its creation and utilization. The utility, productivity, use value and social power of money derive from this organization and can be multiplied without limit by enhancing the quality and reach of that organization. The wider the population covered and the greater the quality, reliability, trustworthiness and accountability of that organization, the greater the power of money. Thus, we see in times of financial uncertainty and political unrest that the value of money can shrink dramatically and even collapse altogether.

Money is a social organization consisting of an intricate network of tangible social agencies. But the reality of money is confined to its external form, structure and economic function. Money is also an intangible social institution that transcends the finite boundaries of the organizations through which it is created and operates. It is governed by informal social practices and conventions, social values and acquired rights, social influence and power that enhance its utility but are not limited by that utility. The hallmark of great speakers is not confined to their vocabulary, the content of their messages, clarity or strength of voice or correctness of grammar. It arises from a sense of trust, confidence, credibility, sincerity, conviction, courage, and strength of personality, logical coherence, idealism, insight, inspiration or other intangible qualities conveyed through the act of speaking. These intangible factors can and usually do exert a far greater influence than the verbal content of the message conveyed. Thus,

Churchill, Mahatma Gandhi and Martin Luther King attracted crowds in the hundreds of thousands and stirred entire nations to act on their words.

The same is true of money. The real power of money derives from the subtle fabric of society which is an unlimited reservoir of knowledge, energy and capacity for creativity and wealth-creation. Money is a subtle force. Like knowledge, it multiplies when it is shared, as Google has grown exponentially to become the most valuable company in the world based on a core strategy of free services to the global public. The immense creativity released since the advent of the Internet two decades ago reveals only the tip of the iceberg of the creative social potential which lies unperceived and unutilized. It was an understanding similar to this that prompted US President Franklin Roosevelt to address the American people on radio as soon as he assumed office in 1933. The country was in the midst of an unprecedented nationwide financial panic that had already led to closure of more than 6000 banks. Nothing FDR had learned studying Economics at Harvard prepared him for handling a crisis of this magnitude. None of the conventional policy instruments applied by President Hoover during the previous three years had been effective. Roosevelt understood that the real foundation of the banking and monetary system was psychological and social. The value of money depends on public trust in the system, the government and the underlying economic system. In his address, he recounted to his audience the great strengths of the American people—their courage, enterprise and ingenuity. He attributed the bank failures to the cancerous spread of fear among the public, which he urged them to reject. He called on his fellow countrymen to act with courage and faith in their nation, by redepositing their hard earned savings in the bank. The following week the panic subsided and the banking system was saved.

Crises arise from opportunities that we are unable to absorb through appropriate social organization, either because the existing system is inadequately developed or because entrenched forces powerfully oppose progress. The Great Depression was not essentially a financial or economic crisis. It resulted from the resistance posed by outmoded institutions and vested interests to a great evolutionary social transition. The New Deal humanized capitalism. It marked a new phase in social evolution, leading to unprecedented growth and prosperity.

Money as Symbol

Organization is an immense power for social productivity. But the power of money does not issue solely from being a social organization. Money is also a mental symbol and symbols possess an extraordinary power of their own that multiplies the power of organization. A 2015 report rated the value of the Apple brand at $170 billion and as the most valuable in the world.[9] The company's logo of an Apple with a bite taken out of it is a symbol that represents not only the company, its products and financial assets, but all the energy, creativity, innovation, glamor and prestige as-

sociated with it. Apple products are a status symbol. A job at Apple qualifies one as a member of an élite group of hi-tech professionals. To sit on the Board or Management Team of Apple opens closed doors around the world. The CEO of Apple can meet any monarch or head of state, even the UN Secretary General or the Pope, just because of his position.

What does money symbolize? At the most basic economic level, money is a symbolic representation of all those things—products, services, technologies, physical and intellectual property, companies, and other forms of capital, etc.—for which it can be exchanged. At a deeper level it symbolizes the economic capacity of the nation that issues and honors it—the natural resources with which it is endowed, the education and skills and enterprise of its people, its physical infrastructure and industrial capacity, etc. Still deeper, it represents the degree of public trust and confidence in the stability of the society and its government, the strength and integrity of its political institutions, its capacity for self-defense and self-preservation, the quality of its educational system, its aptitude for innovation and invention, the value it accords to human life and individuality, its legal protection of property and other rights, and the prevailing cultural values such as those related to freedom, integrity and hard work. The American dollar is accepted today as a *de facto* world currency because it is regarded as a symbol not only for the enormous wealth, resources and productive capacities of its economy, but also for the energy, social organization, individualism, creativity and freedom on which American society is based.

Symbols such as the national flag, the President's seal of office, an Academy Award, Nobel Prize, the policeman's badge, a PhD or MD from Harvard or Cambridge carry far more than utilitarian functional power. The world listens to Nobel Prize winners when they speak, even on subjects for which they have no educational or intellectual qualification. Consumers buy perfumes, watches, designer garments, and sports cars because of the actors and sportsmen depicted in advertisements. Symbols exercise an influence far beyond their utilitarian value.

As a symbol, money can be used to represent many other things, including virtually every type of product, service and material or immaterial asset that is available for purchase or sale in the world. Money also represents other social powers, the capacity for transport and communication, access to education and entertainment, influence over politics, legislation and administrative decision-making, legal recourse to enforce or defend one's rights. Possession of money also carries with it an intrinsic power to access and attract more money. The more money a person has, the more likely it is that others will entrust one with more money. Moreover, the mere possession of money imparts social importance, respect, acceptance and influence over other people which is inherently productive. In combination these powers not only make money valuable and productive, they also make it extremely creative. Money has the capacity to create new opportunities and circumstances, to bring together and com-

bine people, resources and organizational capabilities in innovative ways, to promote the discovery of new knowledge and development of new technologies.

None of these symbolic powers of money is adequately described or explained by conventional economic theory. Nor are they effectively harnessed and utilized for public good by the application of conventional economic policy. But, all of them contribute tangibly and immensely to the productivity and catalytic role of money and its capacity for multiplication and self-multiplication. Only when the subtle nature and deeper powers of money are fully taken into account can the creative capacities of this unique social institution be fully leveraged to maximize human welfare and well-being.

Human Value of Currency

But the real value of money cannot be effectively judged in any of these terms. The true value of any economic or other social system must be weighed in terms of its capacity to promote the security, welfare and well-being of its people. Similarly, markets should be valued in terms of their capacity to stimulate production and promote mutually beneficial exchange between individuals, organizations and nations. So too, the value of money lies in its role as catalyst to facilitate, accelerate and maximize the harnessing of all available social resources for the betterment of humanity. A monetary system that promotes the security and welfare of a few is no better or fairer than a political system that reinforces the power and privilege of an authoritarian party, a military dictator or an aristocratic class.

The real value of money must be judged in terms of how effectively it serves the fundamental purpose for which it and all other economic institutions have been created—to promote and ensure the welfare and well-being of people. The real value of money cannot be judged in terms of what it can buy. The real value of currency is its human value in service of humanity. By that standard, money, like markets, dismally fails to live up to its social mission. As markets are distorted and biased in favor of the economically and politically powerful, the functioning of money in modern society is subject to a wide range of overt and subtle influences that distort its functioning, impact and influence.

The social power of money to legally and illegally influence public elections, government legislation and administrative policy decisions is universally prevalent to varying degrees. It is utilized to influence government spending and subsidies, tariff barriers, export and import policies, patent and copyright laws, rates of taxation on incomes and payroll, capital gains and wealth tax, defense spending, and environmental protection, to name only a few. It explicitly or implicitly determines the actions of central bankers to favor stability of present wealth over policies to stimulate new wealth, job creation and equitable distribution. It skews public policy in favor of technology and energy-intensive investments rather than human capital-intensive invest-

ments. None of these influences are taken into account in a narrow consideration of money as an economic tool. But all of them powerfully influence the ultimate impact of economic policies and activities on human welfare and well-being. A right understanding of money can enable nations plagued by corruption to convert the destructive power of mafia into constructive energies for nation building, on the same principle that inoculations and vaccinations are used in medicine to generate a protective immune response and the repeated assault of viruses and identity theft on the Internet have been used to dramatically elevate the overall level of Internet security.

Signals

Recognition of the wider role of money in society complicates immensely the attempt to reduce Economics to a set of universally valid laws, policy prescriptions and quantitative equations. But efforts to filter out the real complexity of money represent a striking example of what Herbert Weisberg refers to as "willful ignorance."[10] The character of willful ignorance is to collapse reality into a simplistic, manageable set of assumptions detached from the real world and therefore incapable of effectively managing its complexity and uncertainty. Tomas Björkman came to the same conclusion about the models of the market which only vaguely resemble the real world and are most definitely not the only possible or best system we can conceive of.[11]

There are abundant symptoms today of the distorting and confining influence of prevailing economic concepts that prevent us from perceiving, comprehending, seizing and harnessing the fuller productive powers of the global community to promote human welfare.

1. **Multiplication of Financial Assets***:* According to McKinsey, global financial assets have risen 12 fold from a mere $12 trillion in 1980 to about $225 trillion in 2012. Real Gross World Product grew only fourfold during the same period.
2. **Financial Instability***:* According to the International Monetary Fund, in the four decades between 1970 and 2010, there were no less than 145 banking crises, 208 monetary crashes, and 72 sovereign debt crises around the world. This adds up to an astounding total of 425 systemic crises—an average of more than 10 countries in crises each and every year!
3. **Global Savings Glut***:* Although Ben Bernanke alluded to it in 2005 during his term as Chairman of the US Federal Reserve, other economists have been quick to dismiss the notion that there is a glut of money in the world today. He attributed the steep rise in real estate and other asset prices to global surplus savings that are in excess of investment. The onset of the global financial crisis in 2008 lent greater credence to this assertion. While many other explanations have been offered for this phenomenon, the essential fact is that abundance of

wealth generated over the past 35 years is not being optimally utilized to enhance the welfare and well-being of the world's people.

4. **Rising Inequality***:* One obvious reason is the increasing inequality in the distribution of wealth and income globally during this period. Increasing concentration of wealth at the top among those whose consumption needs have already been met to saturation has the minimum impact on growth in global demand for investment in productive assets. This is also associated with rising levels of unemployment globally. In demand-short economies, the greater equity achieved through more progressive taxation means more spending and fuller employment of resources.
5. **Unemployment***:* Rising levels of unemployment globally is another indication that the money is not being productively employed. Today there are upwards of 200 million people unemployed and more than a billion are underemployed globally. This figure grossly underestimates the real deficit. Alternative measures of labor force participation rates in the USA indicate the rate of underemployment is at least double the unemployment rate.[12] According to ILO, the number of working-age individuals who did not participate in the labor market increased by some 26 million to reach over 2 billion in 2015. Vulnerable employment accounts for 1.5 billion people, or over 46 per cent of total employment. In both Southern Asia and sub-Saharan Africa, over 70 per cent of workers are in vulnerable employment. Underemployment reaches as high as 75 per cent in some countries.[13] In a world with a rapidly expanding population and a few billion people at or below the poverty line, there is an ever increasing need for basic goods and services and rising number of people eagerly in search of work opportunities to generate the incomes needed to obtain them. The mismatch between surplus money and productive capacity and unmet human needs signals a dysfunctional financial system. Under these circumstances, greater equity achieved through more progressive taxation would result in more spending and fuller employment of both human and financial resources.
6. **Global Casino***:* Another reason for the global savings glut is the rapid growth of global casino capitalisms following deregulation of banking in the 1990s. This was supported by the fact that companies with strong profits and cash flow accumulated huge cash hoards, rather than increasing investments for business development.
7. **Divorce of Financial Markets & Real Economy***:* Foreign currency exchanges exceeded $5 trillion per day in 2015, fourfold higher than they were 20 years ago.[14] It has been estimated that only 2 or 3 per cent of these fund flows is related to real trade or investment; the remainder 97 per cent takes place in the speculative global cyber-casino.[15] The real economy thrives on stable, predict-

able price levels and stable sources of long and medium term investment. Financial markets have become increasingly divorced from the real economy. An increasing proportion of capital is circling the world in search of speculative returns unconnected with the real economy. Originally established as an effective means to pool the huge amounts of capital needed to support international commerce and industrialization, today computer driven financial markets specialize in leveraging minute differences in prices for fractions of a second. Hedge funds place huge short term bets on exchange rates and asset prices, leading to increasing instability. After deregulation even banks enjoying the support of the central bank joined the bandwagon. As Stiglitz observed recently, "When banks are given the freedom to choose, they choose riskless profit or even financial speculation over lending that would support the broader objective of economic growth."[16]

8. **Rising Forex Reserves***:* The steep rise in global foreign exchange reserves is another indication of a system functioning in highly unstable conditions. Total forex reserves were in excess of $21.7 trillion in 2014 compared to $2.1 trillion in 2000.[17] Countries are compelled to hold higher levels of reserves as protection against the increasing instability and uncertainty of the global market economy.
9. **Negative Interest Rates***:* Money represents productive capacity and social power. An economic system that cannot productively employ the available money to promote economic security, welfare and well-being for all is inherently inefficient and ineffective. In turn, if money does not serve this essential social purpose, then it loses value. One result is the price it attracts in the market place. Today interest rates are negative in economies which account for 25 per cent of global GDP, including Japan, Switzerland, Sweden, Denmark and the Euro area.[18]

Money Myths

The market myths Björkman highlights are not the only myths in town. The gap between our conception of monetary systems and the way they actually work is as great as that which separates economic models of the market from the real world. The gap between the way they work now and better alternatives is equally wide and comprehensible, once we break the conceptual barrier—Canadian Mathematician William Byers' 'blind spots'—that prompts us to cling to distorted images of reality instead of discovering the real thing.[19]

Most of the essential recipes for a more human-centered monetary system are already well known and debated. A tax on short term speculative financial transactions will encourage rather than hamper stable, longer term investments in the real economy. That will help stabilize financial markets which are hypersensitive and un-

predictable. A progressive capital gains tax inversely proportionate to the period of investment would have a similar impact. Eliminating the payroll tax and replacing it with a tax on energy will shift the investment curve from technology to people, removing the artificial bias caused by accelerated depreciation. Reinstitution of progressive income tax rates will support policies conducive to more equitable distribution. Negative interest rates will be a stimulus to both consumption and investment. And so forth.

A more serious objection to reform of monetary systems is the opposition of vested interests and the power of plutocracy, which present serious barriers to reform. The misuse of social power is indeed a real impediment to policy initiatives as it has been throughout history. But that is no excuse for preserving the illusory notion that the present system is either equitable or the best possible. Only when we have the intellectual honesty and courage to squarely confront the truth about money and markets can we hope to change the system. It is time to lift the veil that conceals the underside of society behind the façade of economic theory. Therefore, the concluding section of this paper turns to address the deeper reality so often ignored during discussions of economic theory and policy—the reality of social power.

Social Power

A rational assessment of the present political, economic, social system needs to be founded on an understanding of the underlying reservoir of social potential, how it is converted into effective power, how that power is distributed and how the special interests skew its distribution and usurp that power for private gain. It is thus necessary to develop a vocabulary that distinguishes between the unstructured field of energetic *social potential*, the organized structures and activities wielding *social power*, and the informal mechanisms, both legal and illegal, that result in vast *social inequalities* in the distribution of power and the benefits it generates.

Social Potential

To truly understand the role of social power, we must look beyond the structures and systems that define the formal organized institutional framework of modern society to the infinite reservoir of creative social energies, knowledge, resources and opportunities which represent the zero-point energy field from which all social constructions and achievements emerge. Because it lacks structure, this intangible field of political, economic, social, cultural and psychological energies is difficult to perceive, define, grasp and manage; therefore it is largely neglected by the social sciences which thrive on definition and measurability. Yet this reservoir of power is the source and driving force for social development and evolution and its power exceeds that of the formed society to the same extent as the foundations of an iceberg hidden below sea

level exceed the proverbial tip visible on the ocean's surface. This unstructured amorphous field of society is an inexhaustible reservoir of social potential.

In practice, we are able to grasp the magnitude of that social potential only after it is organized and assumes the form of a social structure. Before the Sears mail order catalog in the 1890s, no one conceived that a company could become the world's largest retailer without operating a single retail store. A century later Amazon repeated that achievement for book retailing in cyberspace, and e-Bay created the first global store in which every consumer can become a merchant. Until Bank Americard morphed into an international credit card system called Visa International a half century ago, no one imagined that electronic credit card transactions could ever replace currency as the dominant medium of exchange. Today global credit card transactions exceed $12 trillion annually. Before Über, no one conceived that a global alternative to local taxi services could be created almost overnight by harnessing the vast unorganized reserve of private cars and car drivers with time to spare and the need for extra cash. Before AirBnB, building a global hotel chain required decades and tens of billions of dollars' investment, because no one conceived that vacant rooms in private homes around the world could be woven in a few years into a global network. Imagine a system that can effectively harness a portion of the world's unemployed and underemployed and you begin to grasp the magnitude of the social potential waiting to be organized.

Social Power

In its widest sense, social power is the capacity of the society to achieve the goals and aspirations of its people. Social power is generated by releasing, directing and harnessing social energies for effective action by creating effective laws, social systems and institutions to organize the diffused energies. Thus, ten thousand years ago migrant tribes of hunter-gatherers evolved into settled communities by adopting a new organizing principle for obtaining food—agriculture. Minute observation of the processes of food production in Nature led them to comprehend the essential role of seeds, water, sunlight, soil and season in food production. They reorganized the entire life of the community to replicate and culture these natural processes. The resulting gains in productivity enabled the world's human population to multiply tenfold.

Social power expresses as the power exercised by individuals. It is the quantum of power an individual can draw from the society as permitted and supported by formal rights, laws, rules and social systems and by informal institutions, customs, usage and values. Each new technology such as the cell phone, each new freedom such as the extension of voting rights, each new law enhancing social security and equality magnifies the power of individuals and of the society as a whole.

Today global society possesses unprecedented and ever expanding power. That power takes innumerable forms: such as the power for transport, communication,

production, exchange, security, governance, education, entertainment, research, invention, discovery and creativity. Over the past half century humanity has witnessed an exponential growth of many forms of social power. Democracy, human rights, rule of law, open markets, entrepreneurship, scientific discovery, technological innovation, globalization, higher education, and access to information have been major drivers of this growth. These gains have led to significant progress in enhancing human security, welfare and well-being, but *the progress has not been commensurate with the potential, because the distribution of the power generated is skewed and biased to favor small economic and political élite.*

Social Equality

Effective power refers to the actual way in which total social power is exercised so as to determine who benefits by it and in what measure. There have always been vast inequalities in the way social power is distributed among the population. In 1880 the 29 greatest British landowners possessed enormous estates. They all had titles; 12 of them were dukes. Fourteen owned more than 100,000 acres each. The Duke of Sutherland, whose holdings were largely in the Scottish Highlands, had well over a million.[20] In addition, this small group occupied the top positions in government, the military and the church. Until 1918, only substantial land owners were permitted to vote in elections. Even long afterwards tenant farmers throughout the country were under obligation to vote for the candidate of their lessee's choice. The higher education needed for social advancement and to gain entry into the seats of power was largely confined to the upper classes. English women only acquired the right to vote in 1932. Needless to say, rights of their overseas colonists were even more limited.

Historical evidence confirms that the greatest social power is generated and the greatest social welfare achieved when the benefits of social advancement are widely and equitably distributed. Modern democracies are far more politically powerful than the monarchies and feudal societies of the past because they are able to more effectively release, direct and channel the energies of their people through freedom and rule of law. Similarly, market economies achieve greater productivity and wealth creation by empowering a much wider section of the population to freely and productively engage in commercial activities.

By historical comparison, the sheer power and productivity of the current market system far excel all previous economic systems. But when the restraints on distribution of social power are fully taken into account, it becomes evident that the present system is far from optimal. There is a vast gap between the total magnitude of social power and the results it generates in society. Vast inequalities in the distribution of social power impact on total social power in the same manner as vast inequalities in the distribution of income and wealth limit the total wealth and prosperity of society. The greater the equality of distribution, the greater the total power generated

and the greater the overall benefit to society as a whole. The total effective power of democracy far exceeds that of earlier forms of governance. So too, the dynamism of the market far exceeds that of centrally planned economies. By the same token, a more equitable distribution of social power would dramatically enhance the overall effective power of society to fulfill the needs and aspirations of its citizens. It is noteworthy that since the collapse of communism, economic theory has remained remarkably silent on this issue, as if the subject were taboo.

The world today has the capacity to provide high quality education to every human being, yet access to education and educational attainments remains far lower and the unequal distribution of wealth is a major reason. The same is true for nutrition, healthcare and other critical needs. Björkman argues that these inadequacies arise from the way in which the market system is being utilized rather than an inherent insufficiency in the system itself.[21] The same basic system can be restructured to generate very different results.

Today the barriers to social equality are prodigious. They take the form of laws and public policies consciously skewed in favor of vested interests, informal support of government for big business, powerful lobbying groups influencing legislative agendas, the influence of money power in elections and consequently on tax policies favoring the rich, along with more overtly illegal forms of corruption and crime that usurp public power for private benefit. Today more than one hundred countries function under the rubric of democracy, yet they vary enormously in the manner in which they elect officials, protect human rights, empower individual citizens, enforce rule of law, legislate and execute policies, etc. A plutocracy or oligarchy masquerades as democracy in some places where huge amounts are spent legally or illegally influencing the outcome of elections. In others a corruption of political power confiscates public wealth for private purpose. Law too preserves an unequal playing field in the form of tax loopholes for the rich, extended patent and copyright privileges, and countless other distorting influences. None of these distortions are essential to the functioning of democracies and market economies, but they have an inordinate impact on the social consequences of the way the systems operate. Yet they are largely ignored and unnoticed.

The distribution of social power has been radically altered over the past few centuries. Monarchy has given rise to democracy, slavery has been abolished, feudalism and serfdom have disappeared, imperialism and colonialism have been supplanted by national self-determination, women and minorities have made great strides toward more equal rights, the blatant aggressive exercise of superior military power—once prevalent throughout the world—has lost legitimacy and is in the final stages of decline.

Historically, all progress has been through violence. Democratic revolution shifted power to the people. Radical shifts in social power have been the result of violent revolutions as in America, France, and Russia and wars of total destruction as

the American Civil War, the two world wars and wars of national liberation. It is only during the last seventy years that we have witnessed peaceful social revolutions of enormous magnitude, as in America's New Deal, India's Freedom Movement, the American Civil Rights Movement, the end of Apartheid, the fall of the Berlin Wall and collapse of the Soviet Empire. Still the threat of violence loomed as a very real force threatening to burst through if peaceful means proved ineffective. Fear of communism was a powerful motive for the humanization of American capitalism under the New Deal.

Thus, the violence avoided by Gandhi burst forth as communal conflict immediately following India's Independence. The Occupy Wall Street Movement of a few years ago is only a reminder that the further distribution of social power is an evolutionary compulsion that is inevitable. The collapse of communism resulted in a temporary lull in the pressure for social equality, enabling reactionary economic thought to regain respectability. But this lull can only be temporary and when the next reaction comes it is likely to be far more powerful and effective when freed of the obvious limitations of authoritarianism that undermined the credibility of communism.

Today powerful vested interests violently support widening economic inequality, which is a legalized violence of the rich and powerful which has to be outlawed to enfranchise all. Historical precedent is no justification or rational basis for the future persistence of social injustice. It is time for economic science to fully acknowledge and impartially examine the underlying fabric of social forces and processes governing the operation of economy today.

Human-Centered Economics

What is Economics? As Political Science is conventionally described as the science of governance, Economics has been traditionally conceived in terms of production, exchange and consumption of goods and services. But it is evident that these descriptions are far too narrow and self-limiting to reflect social reality today. Governance today relates to the entire gamut of human needs and aspirations, from securing the nation's borders and the physical security of citizens and their property to upholding individual rights, promoting social harmony, meeting minimum needs, developing the economy, managing the national currency and budgets, ensuring economic opportunity and security, safeguarding and improving public health, providing quality education, protecting the environment, and countless other activities designed to promote the greater welfare and well-being of all its members.

Democracy is the best means so far developed to accomplish these myriad objectives and it has proven immensely more successful than feudalism, monarchy, military dictatorship and other forms of authoritarianism. At its core, the objective of modern democratic governance is to guarantee basic rights and foster the fullest possible development of the potential of every citizen. Democracies thrive in the measure

they are successful in releasing the energy of citizens and providing them with the knowledge, skills, organizational infrastructure and conducive atmosphere needed for their free, full and creative expression. The right to vote and choose a representative government of, for and by the people is a mechanism developed to achieve maximum protection of human rights and equality before the law. But, ultimately, the accomplishments of democracy depend on its capacity not only to protect and permit but also to actively support and foster the fullest possible development of the capacities of each individual.

The great humanistic psychologists of the later 20th century described the self-actualizing individual as a person able to think for oneself, choose for oneself, rely on one's own capacities, and act freely to realize one's highest aspirations, while respecting and supporting the equal rights of others and accepting the responsibility to contribute to the security, welfare, well-being and fullest development of the entire community. This conception of mature individuality contrasts with the much narrower, one-sided individualism embodied in the phrase 'every man for himself.' The greatest strength of democracy is its capacity to foster the development of individuality in its members.

By extension and necessity, the ultimate purpose of Economics must be the same. Although focused on the economic dimension of human activities, economy permeates and exerts a powerful determinative influence on every aspect of social existence. Freedom has little meaning in a country where people lack economic access to food, housing, mobility, information, education and other goods and services. Freedom without job opportunity and an ensured source of income is like dangling a carrot in front of a horse just out of reach. Economies thrive in the measure they release the energies of their people, channel them in protective activities, and develop the capacities of their members to contribute productively, dynamically and creatively. Here too, individuality is the key. It is the very essence of the entrepreneurial spirit that manifests in the capacity to think and act creatively with self-confidence and courage in pursuit of unrealized opportunities.

The individual plays a unique role in the development of society. Individuals are the birthplace of the rising aspirations, creative ideas, inventions, organizational innovations and dynamic initiatives that characterize a vibrant productive society. The individual is the most precious form of capital any society possesses and the source of its highest achievements. A truly human-centered science of Economics dedicated to the fullest promotion of human welfare and well-being reaches maturity when it conceives and supports measures designed to promote the greatest well-being and blossoming of individuality in all.

Individuality is the basis and ultimate source of social power. Social power is a measure of individual empowerment. Confiscation and seclusion of power as in income and wealth inequality and high unemployment disenfranchise and disempower

both the individual and the society. A true science of economy must encompass these wider social and psychological dimensions.

Notes

1. Eugen Weber, *From Peasants into Frenchmen: The Modernization of Rural France 1870-1914* (Stanford: Stanford University Press, 1976).

2. Adam Smith, *An inquiry into the nature and causes of the Wealth of Nations* (New York: The Modern library, 1937).

3. Anders Aslund, *How Ukraine became a market economy and democracy* (Washington, DC: Peterson Institute for International Economics, 2009).

4. "A Question of Utility," *The Economist*, 8 August 2015, http://www.economist.com/node/21660559; and "Time to Fix Patents," *The Economist*, 8 August 2015, https://www.economist.com/printedition/2015-08-08.

5. Devin Helton, "Great Problems: An Epidemic of Rent-seeking," *Devin Helton* (blog) 14 April 2013, http://devinhelton.com/2013/04/14/rent-seeking-economy/.

6. George F. Will, "It's time to break the teeth-whitening monopoly," *The Washington Post* 10 February 2016, https://www.washingtonpost.com/opinions/is-this-the-end-of-judicial-review-of-economic-regulations/2016/02/10/cb2b6788-cf49-11e5-88cd-753e80cd29ad_story.html

7. L. Randall Wray, "How to Implement True, Full Employment," paper presented at World Academy of Art & Science Global Employment Challenge e-conference, 2009, http://worldacademy.org/node/1748.

8. Tomas Björkman, *The Market Myth*, (Stockholm, Sweden: Fri Tanke, 2016).

9. Nathan McAlone, "Apple is the most valuable brand in the world - for the third year in a row," *Business Insider*, 5 October 2015, http://www.businessinsider.in/Apple-is-the-most-valuable-brand-in-the-world-for-the-third-year-in-a-row/articleshow/49231972.cms

10. Herbert Weisberg, *Willful Ignorance: The Mismeasure of Uncertainty* (New Jersey: John Wiley & Sons, 2014).

11. Björkman, *The Market Myth.*

12. Bureau of Labor Statistics, *Alternative Measures of Labor Underutilization for States, 2015 Annual Averages* (Washington, DC: Bureau of Labor Statistics, 2015), http://www.bls.gov/lau/stalt.htm

13. International Labor Office, *World Employment Social Outlook 2016* (Geneva: International Labor Office, 2016), http://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_443480.pdf

14. Anirban Nag and Jamie McGeever, "Foreign exchange, the world's biggest market, is shrinking," *CNBC*, 11 February 2016, http://www.cnbc.com/2016/02/11/reuters-america-foreign-exchange-the-worlds-biggest-market-is-shrinking.html

15. Bernard Lietaer, "Beyond Greed and Scarcity," *Yes Magazine*, 30 June 1997, http://www.yesmagazine.org/issues/money-print-your-own/beyond-greed-and-scarcity

16. Joseph Stiglitz, "What's holding back the world economy," *Market Watch* 12 February 2016, http://www.marketwatch.com/story/whats-holding-back-the-world-economy-2016-02-08.

17. "Total Reserves (Includes Gold, Current US$) | Data," World Bank, http://data.worldbank.org/indicator/FI.RES.TOTL.CD

18. "Negative Creep," *The Economist*, 6 February 2016, http://www.economist.com/news/leaders/2169 0031-negative-rates-club-growing-there-limit-how-low-rates-can-go-negative-creep

19. William Byers, *The Blind Spot: Science and the Crisis of Uncertainty* (Princeton, NJ: Princeton University Press, 2011).

20. Robert Blake, "Never Has So Few Owned So Much," *The New York Times*, 4 November 1990, http://www.nytimes.com/1990/11/04/books/never-has-so-few-owned-so-much.html?pagewanted=all

21. Björkman, *The Market Myth.*